

# Extracting value for corporate banks from blockchain

The Experts Viewpoint



# Contents

---

03 Blockchain talk

04 Why blockchain, why now?

06 What use cases are we seeing on the blockchain now?

07 Privacy is paramount in banking, but how is it addressed with blockchain?

10 There may be a need to edit the blockchain, but is it feasible?

11 Reviewing blockchain hacks, should banks be concerned?

13 What technology must be obsolete to extract blockchain value?

14 When should banks start preparing for blockchain?



## Blockchain talk

Last month, during Sibos<sup>1</sup>, a group of senior managers from large banks and Fintechs came together for a discussion around blockchain.

Chaired by Ben Robinson, Chief Strategy and Marketing Officer at Temenos, the session was led by a panel of eminent industry experts<sup>2</sup> from ABN Amro, Ripple, Deloitte, Inpher and Temenos, who discussed blockchain feasibility, the tangible value it could offer and its possible use cases. This is a summary of the discussion.

1) Sibos is the world's premier financial services event. Sibos is the annual conference, exhibition and networking event organised by SWIFT for the financial industry.

2) Patrick Stutvoet (Head of Transactions at ABN AMRO), Daniel Aranda (Managing Director, Europe at Ripple), Patrick Laurent (Partner at Deloitte), Jordan Brandt (CEO at Inpher), Darryl Proctor (Universal and Transaction Banking Product Director at Temenos).





# Why blockchain, why now?

Financial institutions' (FIs) profits are under pressure. Interest rates are low and new competitors are squeezing margins. To survive FIs must find more efficient methods to manage and maintain their infrastructure. Blockchain is a major technology for transforming a bank's operating model. From a corporate banking perspective, it offers the opportunity for not just survival but, for those that grasp it quickly and effectively, the opportunity for greater success. Why?

## The trade finance opportunity

At present, when a corporate makes a payment there is almost no information regarding the recipient, what goods or invoices they are for, or when the funds will ultimately be available. These factors limit the predictability required for forecasting and forces finance and accounting departments to be reactive instead of proactive. The process of collecting, verifying, and transferring remittance information, invoices and receiving reports between multiple parties (sometimes millions for larger corporates) is a considerable challenge, and creates significant risk for the FIs. Blockchain provides a means to reduce this risk. It offers the ability to securely connect previously siloed trade finance participants, providing transparency of the supply chain and a massive reduction of manual processes and co-ordination between institutions. How?

A blockchain-based trade network allows information and business logic to be connected

directly to the payment rails themselves. Overcomes the limitations of a correspondent banking network, where remittance data is limited to the few lines included on a Swift message. It allows you to programmatically tie business logic, digital assets and payments together on one platform and automate their transfer based on predetermined digital inputs. And corporates are already seeing the benefit. In a recent survey conducted by Ovum and Temenos, to 200 corporate treasurers<sup>3</sup>, two thirds of the respondents globally were "interested in solutions based on blockchain technology to reduce trading risks".

3) Understanding today's Corporate Treasurer, The implications for corporate banking services, Report by Temenos and Ovum, September 2016

## Connecting the supply chain

Connecting siloed parties also massively reduces the co-ordination and operating costs of trade finance related to the collection of onboarding/ compliance documents and remittance data. Instead of manual co-ordination of these documents along with the necessary payment instructions between the three disconnected participants, payments are routed based on real-time asset ownership information on a distributed ledger. Buyers pay their bills as they normally would, and the funds are routed to the bank, factor or other financier who has purchased the invoice. As you begin to add digital contracts into the blockchain (smart contracts<sup>4</sup>) that trigger under specific conditions, businesses can execute supply chain operation and take advantage of automated financing as needed. In the words of Patrick Stutvoet, Head of Transactions at ABN Amro: *'In providing a true transparent picture of the trade or transaction, the risk associated with collateral can be reduced. The technology allows for the appraisal of the collateral, providing a true insight to know when to execute the transaction etc. thus helping to diminish cost'.*

## Blockchain for factoring

Equally, blockchain is being suggested as way to streamline and de-risk the factoring business, where banks advance funds to the seller of goods or services before the buyer has paid for them. This is another cumbersome process that involves manual checking and opportunities for fraud, and could be made more efficient by a single, distributed ledger including smart contracts.

## Blockchain supporting payments

Earlier this year Deloitte commissioned a survey<sup>5</sup> to financial institutions across the globe to understand how Financial Services are reacting

to the blockchain revolution and a staggering 60% indicated that remittances on the blockchain was an area that banks are looking to focus on. Blockchain technologies, like the Ripple Protocol, enable the creation of the lower cost system that banks need to compete. Because these systems use a distributed ledger approach, banks can utilise real-time settlement (RTS). This lowers the administrative and opportunity costs associated with the current correspondent banking system and as a result, customers can be retained.

"Remittances on the blockchain as an area to focus on"

60%

of Financial Institutions interviewed in a Deloitte survey showed interest to look into

4) Smart contracts are self-executing programs embedded in the blockchain that automatically permit the next step in a process to take place once the necessary conditions have been met and set out the penalties that will apply if the conditions are not met. In principle, incorporating these self-executing, condition-based programs into a private blockchain would enable essential steps in a transaction that today have to be validated and actioned by an intermediary to be completely automated.

5) Blockchain from Hype to Prototype out of the blocks, Deloitte Survey, May 2016

# So what use cases are we seeing on the blockchain now?

During the panel, Daniel Aranda from Ripple highlighted that of the hundred banks today they are working with, around 30 of them have already transacted/implemented real money against payments through their core banking systems or some kind of payment hub systems, moving real money. 10 of these 30 banks working with Ripple are already moving towards moving into commercial production, building of real-time Ripple payment services around their capability centre on the Ripple platform. These banks will soon be able to offer the service to their clients, whether in the retail space, institutional space or the corporate cash management space.

Following on from the success of a proof of concept using Ripple Gateway technology in May, [Ripple and Temenos worked together to integrate the Temenos payment platform with Ripple's core payment solution, Ripple Connect](#). The integration demonstrated that financial institutions using Temenos Core banking software can quickly and easily send payments, either in local or foreign currency, in real-time without relying on intermediary banking relationships and was demonstrated during Sibos 2016.

So, we are seeing proof of concepts related to international remittances, but Patrick Laurent from Deloitte also sees major blockchain opportunities in capital markets where everything except probably the exchange itself will be impacted by DLT. However, even if important proof-of-concepts or even pilots in this space are announced every day, he doesn't expect to see major move of assets to those new platforms before 4 or 5 years. He highlighted that Deloitte recently undertook a proof of concept for

regulatory transaction reporting using Distributed Ledger Technology (DLT). The solution addresses current and future regulatory challenges of OTC transaction reporting from EMIR to MiFIR and SFTR. The counterparties of the transaction will seal and report their deal using a smart contract, whose terms include all the aspects needed for the transaction reporting. The regulators will be able to control and monitor the transaction data and their daily updates, which are stored in the distributed ledger. Deloitte sees its role in the process as supporting counterparties as their agent in validating their data and in setting up and monitoring the smart contracts<sup>6</sup>. And this solution is ready to be deployed now.

But without banks, proof of concepts (POCs) cannot move forward. Many banks are already driving this, such as ABN Amro, with their successful "Blockchain Tribe" innovation group championing many POCs, including a recent one for trade finance contracts.



1/3

of banks working with Ripple are moving into commercial production

<sup>6</sup>) <http://www.financemagnates.com/cryptocurrency/innovation/deloitte-tests-blockchain-smart-contracts-for-emir-transaction-reporting/>





# Privacy is paramount in banking, but how is it addressed with blockchain?

Initially with blockchain there was a very obvious conflict because many of the early blockchain implementations were large, public systems that were publicly available and that's actually really interesting. Anyone in the world with an internet connection could take an API and link up into it. And we have seen various iterations on this in terms of new hashing techniques, as well as private implementations of blockchains.

## An alternative approach to the public chain

Daniel Aranda from Ripple was quick to point what they think is really important about what a blockchain can do; *'it is fundamentally about interoperability. It's about connecting different systems around the world and there is this concept of blockchain enabling an internet of value, where today we have an internet for our communication and data, and that these new technologies and protocol will enable value to move as easily as information does today.'*

He added, *'And at Ripple, when we are sitting around with our product and engineering team, we take some of those analogies like very seriously and almost very literally in a way, and we really think it's about letting different databases of value, essentially ledger systems, be able to connect with each other, communicate and interoperate more*

*efficiently. And a lot of that can be done through cryptographic standards that don't necessarily need to be on a completely public chain.'* Ripple have clearly made progress in this field; *'Something we've been very heavily involved in is a new protocol called Interledger. We are contributed to it within the W3C, which is the standard setting body for the web, and this is essentially a cryptographic standard to allow for two different databases to match a debit on one side with a credit on the other. And it's something that we've been rolling out into all of our solutions but it does allow for, among other things, complete privacy between two transacting parties.'*

So privacy may be possible through a public chain but can it be truly trusted?

..



## The private chain and changing the trust model

Jordon Brandt from Inpher highlighted that the privacy issue is tightly coupled, though not synonymous, with trust. There is a potential threat of that trust model because of the consolidation of those who are actually validating the transactions. One alternative to that is the private chain, even though there's some susceptibility to corruption. He believes that *'we have to look at the fundamental technologies that enable blockchain to operate and I see these as the internet and cryptography. And if we don't get too obsessed with a shiny bubble that's sitting at the surface, you can think of an analogy to the year 2000s bubble of e-commerce. What was lacking in e-commerce in 2000 was the fundamental issue of trust between the purchaser and the seller.'*

Jordon added that *'now we have very standard implementations of SSL and cryptographic protocols that enable us to trust between the buyer and the seller. Obviously e-commerce is now firmly established and we're not going back. And I think some of the same issues are challenging broader adoption of blockchain implementations today. If we look at these fundamental technologies and what's changing in the cryptographic world, there's a lot of innovations happening. Interledger being one, and the other in which we're operating in is what happens when you can compute encrypted data. This means that I, as an individual, have sensitive information, whether it's financial transactions or even my genetic data, and I can trust a third party to compute that on my behalf, without them knowing anything about the data itself. This really changes the idea of the trust model and I don't need to trust a third-party. I don't need even a distributed trust model.'*

## The need for a digital ID infrastructure

However, Patrick Laurent from Deloitte was quick to point out that *'we are missing the digital ID infrastructure where all private data would be secured and self-managed mostly, by the citizen themselves or the users or the clients themselves. This digital ID is an enabler for any type of digitalization.'* Blockchain can have a very important role in the building of this digital ID and authenticate clients or users who are part of the process. However, this piece is not there yet. There are plenty working on the concept but there is nothing universal, at least not at sufficient scale to enable a new digital era supported by blockchain. Patrick added that this was *'the key component. Privacy will probably be structured around those digital ID curl, which is paramount for whoever has to share or to put data into something public. They need to be public if you want to completely leverage the advantage of blockchain and digital concept in the future.'*





## Considering regulation

However, to progress we must consider the regulator. They need to understand the security, understand the digital ID etc. before they can give banks the authority to have a public blockchain and transact on it. Jordon from Inpher reinforced this *'the best way to stay private, currently, as a participant in blockchain, whether as a buyer, a seller or even a minor, is creating a new wall every time you want to do a transaction. That lack of persistence obviously is in conflict with the regulator. They need to know the other end of the transaction ultimately, for an audit. So, there's a striking contrast there between the need for digital ID, but the current method and paradigm of maintaining privacy.'* In addition, regulators need to understand who the actors is ie. is it a good player is a bad player? Are they going to be good at the beginning and then become bad.

Data ownership is also a consideration from a regulatory perspective, particularly with new regulations such as PSD2<sup>7</sup> and GDPR<sup>8</sup>. One area not fully explored is the impact on the blockchain in terms of the right to be forgotten etc. Elements that are very incompatible with interoperability. This requirement to address immutability has perhaps led to the recent announcement that Accenture has designed a distributed ledger platform to enable data to be edited on this blockchain. The prototype according to Accenture is immutable to its user base but, if necessary, designated administrators can "edit, rewrite, and remove blocks of information but only under "extraordinary circumstances."<sup>9</sup> Darryl Proctor from Temenos highlighted however that **if we are going to enable an immutable ledger then blockchain technology (and those operating it) need to be regulated really heavily before they can edit the blockchain.**



7) The Payment Services Directive[1] (PSD, 2007/64/EC) is an EU Directive to regulate payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA). The Directive's purpose was to increase pan-European competition and participation in the payments industry also from non-banks, and to provide for a level playing field by harmonizing consumer protection and the rights and obligations for payment providers and users.

8) The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU. The Commission's primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

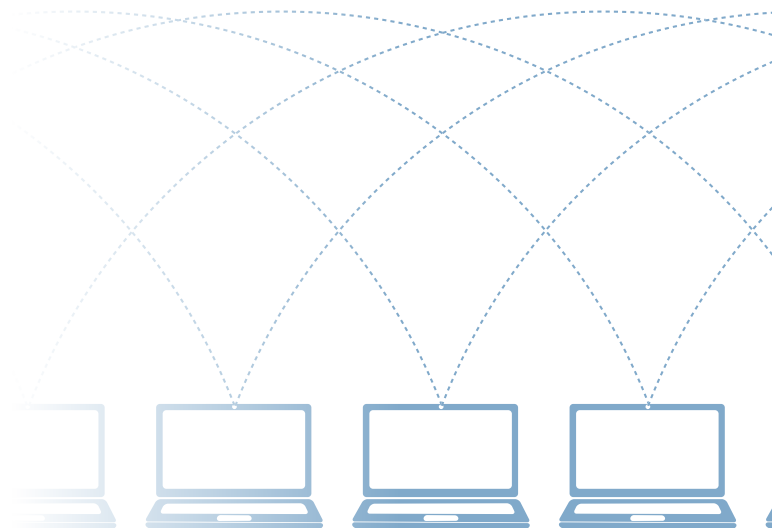
9) <https://www.cryptocoinsnews.com/accenture-unveil-editable-blockchain-prototype/>

# So there may be a need to edit the blockchain, but is it feasible?

Wikipedia is a good example of how this might work. Think about that as an experiment and it generally works quite well right, because it's self-regulated, everyone has a right to edit, but there's a consensus on "are we going to validate that edit or not?". It requires mutability for it to stay true. Jordon from Inpher, highlights an analogy: *'In a way, you are rewriting history, a historical article there and there may be some new fact that is exposed and a need to rewrite Wikipedia. There's a consensus-based idea behind that'*.

Darryl from Temenos has previously highlighted that *'another consideration is who pays for such function? If it's the banks, then they have the right to change what once immutable, but this cannot be. The admins should be completely independent and sponsored only by funds that do not originate from any bank or will not have the ability to influence a change. The change would need to be proven and justified, by all parties in said transaction'*<sup>10</sup>.

However, the risk of misuse in the blockchain are far greater than those we see when wiki is mis-edited. For example allowing editing leave an open for door to cyber-attackers. These concerns may outweigh any argument that a blockchain needs to be edited in case of human error and perhaps should be addressed outside of the blockchain i.e. before the information is committed. It seems counter-intuitive that risk and regulatory requirements would make "absolute immutability a potential roadblock" for banks, when trust in the transaction record chain would seem to be fundamental to evidence of compliance.



<sup>10</sup>) Blockchain in Banking LinkedIn Group discussion, Accenture's Plan to Edit Blockchain Is Causing Some Controversy, September 2016



# Reviewing blockchain hacks, should banks be concerned?

Every week we hear of some new blockchain hack. However, as Patrick from ABN Amro highlighted, most believe the blockchain is secure enough. The technology is there, but we should never pretend that something is completely secure. One of the key rules in banking should be to never assume that your system is fool proof. Someday your system will be hacked. Patrick added *'at some point in time your blockchain will be compromised and then who's accountable? For example, when we had the issue with the banking cards that could be copied, the banks took the responsibility and basically paid people who lost money. The trust wasn't deteriorated in the system; the system was still trusted.'* So we must consider who is accountable if/when the blockchain is compromised.

Many of the examples of hacks we are seeing are from inadequate solutions and related particularly to cryptocurrencies at the moment. There is for example, vulnerability in having a chain with very few nodes. This makes for an easy target for someone to attack the chain as there were no other security mechanisms in place. **When bitcoin began**

with just a handful of nodes their tokens had the value of a fraction of cents, so it was economically unfeasible to attack them. However, as the network grew the value of bitcoins grew. While they are at a decent value today their network is at a size that makes an attack economically unfeasible - you'd simple burn more money on electricity than the bitcoins that you can steal are worth and at the same times the bitcoins you've stolen would become less valuable as the network has to assume stolen tokens. As long as this equilibrium of value and potential to hack remains intact the risk of an attack on blockchain technology and particularly cryptocurrencies employing POW algorithm, is low<sup>11</sup>.

11) Content from a discussion with Peter Koen, Senior Director, Timezone Lead EMEA, Azure Customer Advisory Team at Microsoft on Blockchain Banking LinkedIn Group, September 2016



# So with hacks a low risk, how long until the industry feels comfortable with blockchain?

There is an analogy with when cloud was first introduced into the banking environment. Patrick Stutvoet from ABN Amro, highlighted that initially banks only wanted to use private clouds. And bit by bit they are becoming more comfortable with using the public cloud. And as with cloud, regulators will become more confident about blockchain as concerns around security are overcome. So with

blockchain, it may start as permission based, banks will form consortiums, and once they have started to extract value, they may ultimately move to a public blockchain because that's the only way you can really make this truly democratic.

## And looking at blockchain standards, how do you all see this evolving?

*'There are new innovations happening that are foundational to what has enabled blockchain to happen. It may perhaps be foolish for us to believe that what we see now is going to be the ultimate iteration of this. We must consider that as the internet evolves, and accessibility to it evolves, is everyone participating equally in this new operational environment?' Jordon from Inpher adds, 'If we're just seeing consolidation that means it doesn't matter if the 'man on the street' connects with a new node in South Sudan, they can't participate. For example, effective today, if someone plugs in their laptop they can only currently perform transactions. They can't participate in the validation today effectively, because they don't have a supercomputer that's purpose-built for mining and doing a proof-of-work algorithm. Blockchain should be inclusive. In order to do that, people have to ensure the privacy issue. And for banks to ultimately have trust they need to understand the fundamental technologies quite well.'*

for complex process handling and multi-party process handling. Some can use and already use public blockchain and some other would-be already fully framed within the private block chain. Patrick from Deloitte was quick to highlight that we must consider if these different strains should communicate. *'Surely how blockchain technology in-house, in logistics, in plenty of domains where they're payments attached to some transactions or some moves of goods communicate has to be tackled. At present there are not that many private blockchains which are in production which could communicate with each other, however, once more use cases and live scenarios are available this discussion must be had.'*

### Connecting different blockchains

Different use cases will use different blockchain technology. Some strains of blockchain are suited to scale, supporting huge, very simple transactions, whereas smart contracts on ethereum are designed

# So what technology needs to be made obsolete to extract the value of blockchain?

*'Blockchain is basically real-time' Darryl from Temenos highlighted 'In terms of payments, many of the old systems are batch based. There has to be a technology change, there has to be a transformation from these legacy systems, these monolithic blocks of technology, into more modern open architecture. Architecture that can deal with real-time and operate 24 x seven.' And of course, all banks will need to have systems to manage real-time payments so the need is twofold.*

However, we must remember that **blockchain technology is a layer outside of a bank that they must interact with. But banks must have agile systems to interact with blockchain services.**

But as well as having the right technology within a bank we must also consider blockchain technologies that won't survive. Jordan from Inpher highlighted this: *'the reality is that you need the redundancy even amongst blockchain technology. That's a reality we're going to the deal first of all; that with all the different that hundreds of different ecosystems we see rising we always want a single source of truth to go after. We can't discount the reality of the other one.'*

Banks must have agile systems to interact with blockchain services

# When should banks start preparing for blockchain?

There is a consensus that blockchain adoption by banks will be within the next five to seven years. We will move from current POCs to production pilots in the next year or so. This approach was reinforced by ABN Amro confirmation that they are moving their Trade Finance POC into production over the coming year. And this bank focus on blockchain isn't unique to ABN Amro, Darryl from Temenos added that *'Even from a Temenos perspective, we have 2000 plus clients and almost every single day I get a query around 'how do I implement blockchain with your software?' So blockchain is here now and banks are working on it.'*

Patrick from Deloitte reinforced that there is an opportunity now. Although *'the big shift in assets, considering capital market as a whole, moving to blockchain will not happen overnight. However, it doesn't mean that you have to wait for capturing value from this technology. We have seen so many proof-of-concept over the last two years, that it's time to go to production now; that's the key message.'*

Patrick went on to highlight that the process of blockchain adoption might be accelerated if centrals issue central bank money on the blockchain. *'If this move comes the advantage of this is obvious; the accelerations would be extremely huge. Most central banks are discussing this possibility and that's a real advantage we can you can imagine over the next year or even months.'*

So the answer as to 'when should banks start preparing for blockchain', is that they should already have started. The only thing that's stopping them is having the right relationships, the right strategy and the right infrastructure to make this most of this disruptive technology.

Jordon Brandt from Inpher, crystalised what banks need to do in his final comment *'you have to embrace a culture of iteration. You have to try a little bit, take a little bit of risk. See how it works, because we're not going to get it right first time. It's about enabling people to take quantitative risk and iterate on that to increase the pie; because you're not going to eat it all and move all of your assets there at the same time; that would be a fool's errand.'*

..

Adoption might be accelerated if centrals issue central bank money on the blockchain



Author:

Emma Wadey

Product Strategy

**Temenos France SAS**



TEMENOS™ is a registered trademarks of Temenos Headquarters SA

©2016 Temenos Headquarters SA - all rights reserved.

Warning: This document is protected by copyright law and international treaties. Unauthorised reproduction of this document, or any portion of it, may result in severe and criminal penalties, and will be prosecuted to the maximum extent possible under law.