

# Financial IT

Innovations in FinTech

**TECH HOLDS THE KEY:  
HOW FINANCIAL  
SERVICES  
ESTABLISHMENTS  
CAN FIGHT OFF THE  
FINTECH THREAT**

**Rahul Singh,**  
President of Financial Services,  
HCL

**ISLAMIC FINANCE  
PRACTICES:  
LIMITATIONS AND  
PROHIBITIONS**

**Rosie Kmeid,**  
Vice President, Global Corporate  
Communications & Marketing,  
Path Solutions

**THE FUTURE  
OF PAYMENT  
PARTNERSHIPS**

**Matthias Setzer,**  
CCO, PayU

**TOP 12**

**CRYPTO  
STARTUPS  
TO WATCH  
IN 2019**

**WHAT TRENDS  
SHOULD BANKS  
BE AWARE OF  
IN 2019?**

**Mark Aldred,**  
Banking Specialist, Auriga

Trulioo | GLOBALGATEWAY

Providing financial services to  
Knowing your customer is **ours.**



- Instantly validate company vitals for over 250,000 merchants worldwide
- Run AML/KYC checks for businesses and UBOs in a single workflow
- Real-time onboarding delights customers while satisfying Customer Due Diligence



customers is **your** business.

## Automated Know Your Business Workflow Helps You Meet AML Law

Validate company vitals  
& check against AML list



Analyze ownership  
structure & stakeholders



Identify beneficial owners



Perform AML/KYC  
checks on UBOs



Learn more at [trulioo.com](https://trulioo.com)

# A BETTER WAY OF LOOKING AT FINTECH?

## WHAT REALLY MATTERS IS THAT THE POSITIVE CHANGES THAT ARE UNDERWAY ALWAYS TAKE LONGER THAN EXPECTED.

One of the lead articles in this edition of Financial IT highlights how banks will continue to be excited about Artificial Intelligence (AI) in 2019. There will be experimentation involving AI. There will be investment in AI. However, mainstream adoption of AI solutions are unlikely. This is partly because the demands of clients are complex and increasingly sophisticated. Chatbots may be able to reduce costs and boost efficiency, but they are not – yet – able to provide the tailored customer experience that clients are looking for.

We are at the end of the year which brought the second Payments Services Directive (PSD2), the revised Markets in Financial Instruments Directive (MiFID II) and the General Data Protection Regulation (GDPR) to the European Union (EU) and, indeed, the world. Financial institutions and FinTechs have invested heavily to adapt to the new requirements and to exploit the opportunities from Open Banking. However, it is not yet obvious who has made, or will likely make, the greatest gains.

In spite of much excitement, along with a boom and bust in crypto-currency markets, it is still not clear how what will be the main impact on banks and other financial institutions of Blockchain technology. One of the contributors to this edition of Financial IT notes how several of Canada's largest banks are collaborating to develop customer identity solutions that are based on Blockchain. This is a good example of how institutions that are naturally competitors can work together to use technology to solve problems. However, the problems have yet to be solved.

And problems still abound. As other contributors to this edition note, only 38% of banking and securities leaders have a high confidence in their ability to detect and prevent fraud. In 2018, some 53% of customers of United States-based online retailers abandoned transactions before completing their purchases. Financial institutions are still trying to work out how best to leverage client data that is held in legacy systems.

Broadly speaking, two key conclusions can be drawn from all this. One is that, at the intersection of financial services and IT, the hype often exceeds – or differs from – the reality. In the case of AI, the issue appears to be that robots are, for now, better suited to manufacturing than services. New and higher regulation through the EU's Directives and Regulations increase operating costs, but also barriers to entry – providing additional advantages to incumbents.

The other conclusion is that it not helpful to think of FinTech in terms of single concepts such as Blockchain, AI or Open Banking. Rather, it is better see the combination of financial services with IT as a universe in which positive change takes place on dozens of fronts simultaneously. Problems need to be identified. Technological solutions need to be developed. Institutions and FinTechs need to assess whether they will operate independently or collaborate with each other. The new solutions need to be implemented and evaluated. All this takes time. Change often takes place far more gradually than is envisaged.

FinTech Connect 2018, which takes place in London on 5-6, is structured in a way that recognizes this. Events are organized around several broad and, to a certain extent, inter-related themes. The include: digital transformation; IT and infrastructure upgrades; paytech and the cashless society; regtech and compliance; the evolution of insurtech, and fast growth strategies for start-ups.


We wish all participants at FinTech Connect 2018 – as well as our subscribers, advertisers and contributors – all the best for 2019. It may well be that the real impact of the experimentation and collaboration that is currently underway is only obvious in late 2021 – or three years hence.

*by Andrew Hutchings, Editor-In-Chief, Financial IT*

Follow Us

 **Twitter** @financialit\_net

 **LinkedIn** [https://www.linkedin.com/company/rfp-connect\\_2](https://www.linkedin.com/company/rfp-connect_2)

 **Facebook** <https://www.facebook.com/financialit.net/>

## Financial IT

Innovations in FinTech

Although Financial IT has made every effort to ensure the accuracy of this publication, neither it nor any contributor can accept any legal responsibility whatsoever for consequences that may arise from errors or omissions or any opinions or advice given. This publication is not a substitute for professional advice on a specific transaction.

No part of this publication may be reproduced, in whole or in part, without written permission from the publisher. Entire contents copyrighted. Financial IT is a Finnet Limited publication. ISSN 2050-9855

Finnet Limited  
137 Blackstock Road, London, N4 2JW,  
United Kingdom  
+44 (0) 208 819 32 53

**Founder**  
Muzaffar Karabaev

**Editor-In-Chief**  
Andrew Hutchings  
[andrew.hutchings@financialit.net](mailto:andrew.hutchings@financialit.net)

**Publisher**  
Chris Principe  
[chris.principe@financialit.net](mailto:chris.principe@financialit.net)

**Project Coordinator, Managing Editor**  
Katherine Emirosan  
[kemirosan@financialit.net](mailto:kemirosan@financialit.net)

**Content Editor/Events**  
Nilyufar Sodikova  
[nilyufar.sodikova@financialit.net](mailto:nilyufar.sodikova@financialit.net)

**Content Writer**  
Oksana Pak  
[oksana.pak@financialit.net](mailto:oksana.pak@financialit.net)

**Multimedia Editor**  
Bekhriz Khazratov  
[bekhriz.khazratov@financialit.net](mailto:bekhriz.khazratov@financialit.net)

**Production/Design**  
Timur Urmanov

# INNOVATIVE FINTECH. REAL-WORLD APPLICATIONS.

**1400+** attendees. **65+** firms demoing.  
**120+** expert speakers. Insights and  
connections you only find at Finovate.

**FINOVATE EUROPE**

*Main Conference: February 12-14, 2019*  
*Additional Summit Day: February 15, 2019*  
Tobacco Dock, London, UK

[finance.knect365.com/finovateeurope](http://finance.knect365.com/finovateeurope)

**SAVE 20%** WHEN YOU REGISTER WITH VIP CODE FKV2349FITFA

**KNect365**  
Finance

# CRYPTO: CRYPTO OR A GOLD MINE?

Where would you rather be? In a crypt, or a mine?

As you probably remember, Bitcoin was the dinner table talk and the big news headlines of a year ago. As crypto-currencies had soared in value, it was rightly the dominant topic of conversation.

Crypto-currencies had advanced in value quite dramatically through the second half of 2017, from about US\$1,000 a coin to over US\$18,000 in the case of Bitcoin. This created huge paper profits for many, and had them thrilled. These people were excited and expected the rise in value to continue. The buying frenzy heated up to peak rarely before seen in any investment or commodity. Popular exchanges, like Coinbase, had to cope with the opening of hundreds of thousands of new accounts during the last few months of 2017.

Mobs of speculators were piling in, bidding the price up to new highs on a daily basis, until it almost cracked \$20,000 a Bitcoin.

This generated huge demand for Bitcoin, but no fundamental value. Bitcoin became a textbook example of a speculative frenzy.

At the end of 2017, the outrageous predictions of Saxo Bank included a fall in the price of Bitcoin to US\$1,000 during 2018. There were many similar predictions as 2018 unfolded. That collapse is still possible as we have seen Bitcoin drop to as low as US\$3,500 after a period of price stability in the US\$6,000 to US\$7,000 range. This was as unexpected as it was expected!

Indeed, the fall in the price of Bitcoin has the potential to become a self-fulfilling prophecy. Saxo Bank's outrageous prediction may yet come to pass.

What a difference a year makes.

## Crypto to Crypt

The end of the hype about Bitcoin – and the concept that it could continue to rise – has played into the hands of the crypto-whales. The crypto-whales have had the chance to cash in at a huge profit and cash back in buying at cheaper prices effectively giving them control of more Bitcoins. They now control a huge percentage of the available Bitcoins giving them the ability to

influence the market when and at what price they wish. Today they are at it again, forcing the price down to accumulate at new lows. The crypto-whales sell off: this causes panic sellers to also sell. The price goes down, giving the crypto-whales buy back in at the lower prices and accumulate more. This is classic market manipulation of an asset whose promoters claimed it could not be manipulated.

Those who bought at the high point of the market have now taken such a big loss that they might as well be buried in a Crypto Crypt. Bitcoin is a strong candidate for the title of the biggest financial scam in history – making the wrong that Bernie Madoff did seem minuscule. There is an additional important difference. Bernie's sins hit people who were already wealthy. The manipulation of the Bitcoin hit people who are hardworking and saving types. They had emptied their retirement funds and loaded up their credit cards to make their families lives a little better – and now are suffering terribly.

I know die-hard Bitcoin faithful who finally are selling out, getting whatever they can, while they can. With the value of their crypto assets collapsed by 80%, they still have to service their debts and work to avoid personal bankruptcy.

Is this the end and the only thing left to do is seal the Crypto Crypt? Are Bitcoin and all crypto-currencies headed into history like Dutch tulips and Pets.com?

There are so many worthless coins and tokens out there, and many of them are absolutely headed to zero. Many have been set up as scams from the start and taken advantage of people who are hoping for the next shooting crypto star. These are high-risk companies often run by scammers who are great at turning YOUR money and THEIR dream into THEIR money and YOUR dream.

Bitcoin was the first crypto-currency and the biggest by market capitalisation. At the same time, it is based on inferior technology compared to what is currently available given the advances that the market has made. It is backed by absolutely nothing and useful for next to nothing. That should clearly push Bitcoin to failure and makes little sense that it is the most valuable.

Many argued that crypto-currencies represented a great technology to improve the financial system. The concept is sound where a crypto-currency serves as a medium of exchange not controlled by bankers. It is sound in a world where online transactions are done at low cost. This is the revolutionary idea described in the original white paper a decade ago which became Bitcoin. A crypto-currency may still someday realize this goal. The greater opportunity is the use of Blockchain, Distributed Ledger Technology (DLT), this will change commerce, finance and yes, our own lives.

FedCoin, EuroCoin, IMFcoin, UNcoin, eRuble, CADcoin ... such things will be created. I can see the adoption of private systems for tracking and trading other valuable things – barter done practically using Blockchain. History likely will have people turn back to using real, physical, valuable, anonymous money – GOLD!

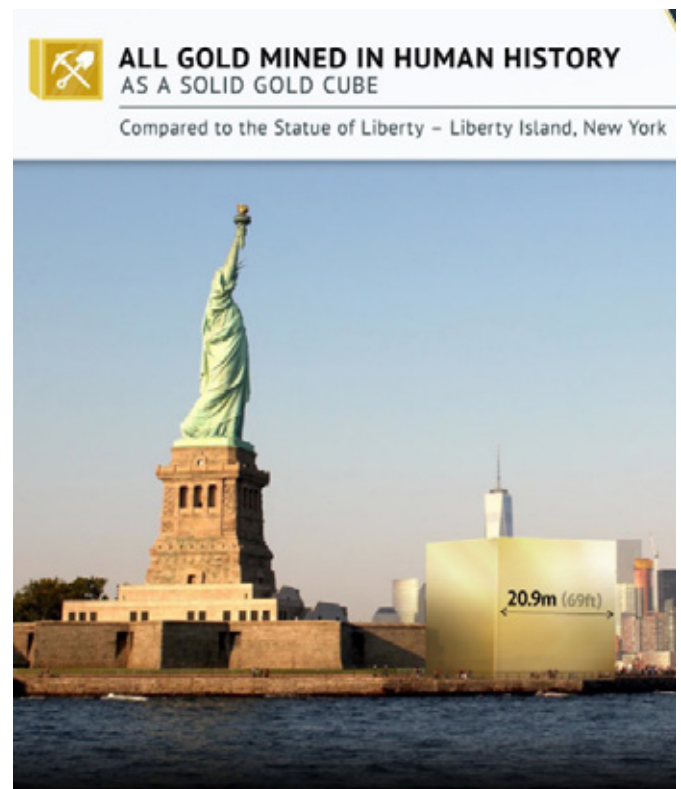
## Own a Gold Mine

Yes, buy a gold mine, seriously. Buy gold, gold coins, and gold contracts. History has proven that this is the only store of value that really works. Since 2013, gold production has decreased each year. There has not been a sizable new gold find since 2014. Supply is decreasing, and demand is there, and the pricing proves it. Gold mining companies are thrilled when they can recover one gram of gold in each ton of earth.

The bottom line is that: gold discoveries are dwindling.

All the gold mined in history, is about 166,500 tons and is divided into four uses. The biggest is jewelry, 50.5% of all gold. It is not necessarily a good investment, but your significant other will love it. Number two is private investment at 18.7%. The third is government holdings with 17.4%, and industry uses 13.4%.

Gold is extremely rare, impossible to create out of “thin air”, easily identifiable, malleable, and it does not tarnish. Gold has been highly valued throughout history for every tiny ounce of weight. That’s why people have used it for centuries as a monetary metal, a symbol of wealth, and a store of value. For thousands of years, gold



has been the safe-haven asset. No government can easily confiscate, nationalize, freeze, or devalue on the word of a politician.

So, when demand for gold really starts to heat up, the supply won't be there. Gold is rare, limited and forever in demand. This will cause the gold price to soar and silver potentially even more. It's simply the best way to preserve wealth over the long term.

Buy a Gold Mine or be buried in a Crypto Crypt!

*Chris Principe, Publisher, Financial IT*



**EDITOR'S LETTER**

- 2 OPEN BANKING...  
...WHAT WOULD HAVE  
HAPPENED IF IT HAD NOT  
ARRIVED IN 2018?**  
*Andrew Hutchings, Editor-In-Chief,  
Financial IT*

**COVER STORY**


- 8 WHAT TRENDS SHOULD BANKS  
BE AWARE OF IN 2019?**  
*Mark Aldred,  
Banking Specialist, Auriga*

**PUBLISHER'S LETTER**

- 4 CRYPTO CRYPT OR  
A GOLD MINE?**  
*Chris Principe,  
Publisher, Financial IT*

**INNOVATION CORNER**

- 12 INNOVATION  
AND COMMODITISATION:  
EXTRACTING VALUE FROM  
THE NEW ERA OF PAYMENTS**  
*Abhijit Deb,  
Head of Banking & Financial  
Services, UK & Ireland, Cognizant*

**LEAD STORY**

- 16 TECH HOLDS THE KEY:  
HOW FINANCIAL SERVICES  
ESTABLISHMENTS CAN FIGHT  
OFF THE FINTECH THREAT**  
*Rahul Singh,  
President of Financial Services,  
HCL*
- 20 THE FUTURE OF PAYMENT  
PARTNERSHIPS**  
*Matthias Setzer, CCO, PayU*
- 36 ISLAMIC FINANCE  
PRACTICES: LIMITATIONS AND  
PROHIBITIONS**  
*Rosie Kmeid,  
Vice President, Global Corporate  
Communications & Marketing,  
Path Solutions*

**INTERVIEW**

- 32 DOSHEX:  
TOKENISING THE WORLD**  
*Alex de Bruyn, CEO, DoshEx*

**INDUSTRY RANKING**

- 45 TOP 12 CRYPTO STARTUPS  
TO WATCH IN 2019**

**FEATURED STORY**

- 10 WHAT THE GLOBAL PAYMENTS  
INDUSTRY CAN LEARN FROM  
COMPARISON SITES**  
*Peter Keenan, CEO, APEXX*
- 14 ENSURING BANKS TAKE THE  
RIGHT APPROACH  
TO DIGITAL ID SCHEMES**  
*Written by Patrick Kleuters,  
SVP Europe, Gemalto*
- 18 UNDERSTANDING THE FACES  
OF BANKING FRAUD –  
IMPROVING DETECTION AND  
PREVENTION IN AN EVOLVING  
THREAT LANDSCAPE**  
*Steven Murdoch,  
Innovation Security Architect,  
OneSpan*
- 22 THE SECRET TO REDUCING  
TRANSACTION ABANDONMENT:  
BEHAVIORAL BIOMETRICS**  
*Noa Benari,  
VP Marketing, SecuredTouch*
- 24 TRANSFORMING THE  
INSURANCE CUSTOMER  
JOURNEY WITH AI**  
*Richard Price,  
Head of Financial Services  
Practice – UK&I, TIBCO*
- 28 ENSURING  
YOUR INSURANCE**  
*Patryk Pilat,  
Head of Pre-Sales Engineering at  
Blueliv.*
- 30 TECHNOLOGY HAS NOT  
HELPED BUSINESSES  
SURVIVE – UNTIL NOW**  
*Simon Lyons,  
Chief Commercial Officer,  
Slide*
- 34 UNDERSTANDING THE  
CONTRACTUAL LANDSCAPE  
KEY TO PLOTTING THE 'BREXIT'  
ROUTE**  
*William Rees,  
Business Consultant, iManage*
- 38 THE BIG TECH THREAT FOR  
FINANCIAL SERVICES FIRMS:  
FIVE COPING MECHANISMS**  
*David Jones,  
VP of Product Marketing,  
Nuxeo*
- 42 CYBERSECURITY SHOULD  
BE MORE THAN A TICK BOX  
EXERCISE, AS REGULATIONS  
ARE ON THE RISE**  
*Dave Locke, Chief Technology  
Advisor at World Wide Technology*





# OPEN

for innovation

It's time for a new way to write, deploy and consume financial software. At Finastra we've done just that, by developing a platform that's open, secure and agile. It lets you integrate new technology seamlessly – bringing new products to market more quickly and with a better customer experience.

As we say, it's innovation with unlimited potential.

( THE FUTURE OF  
FINANCE IS OPEN

Join us at [finastra.com](http://finastra.com)



**Mark Aldred,**  
Banking Specialist, Auriga

Mark currently serves as Head of International Sales at Auriga, a leading European vendor of advanced multichannel banking software. His main role is to support the expansion of Auriga into new geographies around the world. He has over 30 years' experience in banking technology in various management and director roles for companies including FIS and ACI Worldwide.

WHAT  
**TRENDS**  
SHOULD  
BANKS BE  
AWARE OF  
**IN 2019?**





As 2018 comes to a close, the industry is looking to the key trends that will shape the banking industry in 2019 and how they need to prepare.

## Bank branches as digital hubs

In 2018, a key trend we witnessed was the shrinking of branch networks as infrastructure costs, combined with a general decline in usage of bank branches prompted banks to consolidate. There will still be demand for bank branches in 2019 though – according to data from Capgemini, 60.1% of customers rated bank branches as important. In 2019, we will witness banks focussing investment into their remaining locations. In fact, branches are set to become ‘smarter’ than ever before and develop into fully digital hubs.

We will see banks deploying more in-branch technology that improves user experience, including video banking and smarter use of in-branch tablets to improve service and sales. There has been a lot of talk of banks planning completely omnichannel, seamless experiences but next year may be the year we start to see banks achieve this. As customers shift to almost fully digital relationships with their banks, they will demand exceptional user experiences that provide real value.

## Location, location, location

Banks will continue to review their branch networks next year. We are likely to see them relocating away from underperforming locations and opening in areas of higher footfall and with more demand for banking services, such as out of town shopping centres.

We’ve already seen retail banks including Lloyds and Halifax open state-of-the-art branches in Manchester city centre and in central London, and this trend of banks investing in city centre flagships is set to continue, especially as such locations become more accessible as a result of investment in smart cities and improved transport links.

## Open Banking and PSD2

The Second Payment Services Directive (PSD2), which came into force in January 2018, is an opportunity for banks. They may seek to monetise and share their customer data with third parties such as FinTechs and to enable collaboration to create first-of-their kind offerings.

While Open Banking and PSD2 have prompted banks to think about their offerings, progress has been slow so far. The full range of potential threats and opportunities from Open Banking are yet to be realised. This is especially true as the digital natives, who at age 18 are now opening their own bank accounts, try to balance their demand for easy to use, integrated services (such as account integrators and budgeting apps) with concerns around data privacy.

Financial institutions will need to think creatively and capitalise on new technologies to offer the right solutions in the right moment to their customers.

## Collaboration over competition

Competition in the banking industry is already fierce, fuelled not only by the likes of new entrants like Monzo, Starling – and more recently N26 – but also by traditional players stepping up their game by innovating and enhancing the customer experience, challenging the challenger banks themselves. With banks still adapting to the changes set in motion by PSD2 next year though, competition will only intensify.

This increasing competition is spurring banks to develop their offers in order to differentiate themselves and drive growth. However, with customer expectations rising and demands continuously changing, financial institutions are realising the benefits of working together to meet their goals. Through collaboration, customers can get the best of both worlds, FinTechs can expand their offerings, and traditional banks can maintain their share of the market and adopt new services into their existing portfolios. We’ve already started to see this collaboration – Starling recently announced a collaboration with the Post Office to allow cash withdrawals, deposits, and balance enquiries to retail and business clients and Monzo quickly followed using the infrastructure of PayPoint. This leverages the customer experience and journey expertise that challenger banks have put at the centre of their offering, combining it with the infrastructure presence of traditional players.

## More experiments but little likelihood of mainstream AI rollouts

Despite the buzz around artificial intelligence and how it will revolutionise banking, development and deployment of AI in 2019 will broadly remain experimental. More and more, banks are testing AI for easily repeatable tasks, for example using chatbots to administer dialogue between the bank and its customers, and this is resulting in great improvements to system efficiency and cost reduction. In fact, according to the World Retail Banking Report 2018, while AI adoption is expected to lead to \$1 trillion savings, it will take until 2030 by which time operational expenses will have been reduced by 22% as a result. The continued gradual introduction – in a managed way – of AI is something we are very likely to see.

There is much to be excited about over the next 12 months within banking, but also a growing number of challenges market players need to be aware of, especially with rapidly changing consumer expectations of the ideal financial service experience. Banks must be willing to adapt, trial new technologies and collaborate in order to succeed in what will prove to be another highly competitive and fast-moving year for the industry.



# WHAT THE GLOBAL PAYMENTS INDUSTRY CAN LEARN FROM COMPARISON SITES

With card spending equivalent to about a third of the UK's GDP, card payments are critical to the smooth running of the economy. Earlier this year, debit card payments overtook cash as the most popular form of payment in the UK for the first time. Consumers are looking for quick, convenient ways to pay; contactless payments are now more popular than chip and pin card transactions in the UK and we're seeing a sharp rise in the use of mobile wallet payments such as Apple Pay or Google Pay. Merchants spend millions of pounds processing payments every year. But in an industry saturated with merchant acquirers and payment providers, the amount of choice can be overwhelming. Due to this sheer complexity, the global payments market has become opaque, stagnant and ultimately full of complacent providers. So much so that Britain's official payment watchdog group, the Payments Systems Regulator (PSR), is currently reviewing banks that process card

transactions to evaluate whether customers are getting a fair deal.

## What comparison sites did for the personal finance market

The global payments industry can learn valuable lessons from CompareTheMarket and other price comparison sites. Personal finance was transformed as these sites recognised that despite the wide range of choice, consumers weren't switching products and were missing out on massive savings. This stemmed from a lack of awareness as consumers avoided the complex and time-consuming processes of individually comparing and changing providers.

By creating an ecosystem of service providers, comparison sites gave consumers what they had been missing – easy access to choice. Not only did this provide more options, the enhanced transparency in the

market encouraged fierce competition, forcing businesses to innovate and reducing prices as a result.

The global payments market is every bit as complex for merchants – if not more so. Each year, merchants spend millions of pounds processing credit card, debit card and alternative payments with acquirers. This involves at least four parties but can include many more. Understanding which entity does what, why each charges the fees, and if they're charging a fair price, often proves an impossible task for merchants.

## The payments maze

An efficient payments model is vital for business growth, but businesses have been deterred from trying to navigate the global payments maze. As a result, they are unaware of the wealth of options available to them, and because it's crucial to have payments capabilities, they usually select providers as quickly as possible.

If these time-poor businesses were able to explore the market, they would discover that integrating with multiple acquirers can generate huge cost saving on FX and basic payments acceptance and also dramatically increase the conversion rates of transactions. However, with the market as perplexing as it is, finding time to explore its intricate landscape simply isn't a reality.

## Sub-standard services

With the market's complexity, it is unsurprising that once a merchant selects an acquirer, the perceived difficulty of switching often discourages merchants from doing so. As a result, there's little competition and no incentive to innovate, create better services, or lower prices.

Businesses and consumers bear the brunt of this, as services become increasingly outdated. Payment services are not improving fast enough to keep up with consumer expectations for quick and painless transactions, particularly online. Consumer expectations are evolving, and payment services too often don't allow for the efficient and painless online transactions they expect. 70% of online shopping carts are abandoned, while Barclaycard research states that British shoppers abandon online baskets worth almost £30 a month, potentially resulting in more than £18bn in lost sales every year.

## Change is coming

The latest legal battle over interchange fees which saw major UK high street retailers sue Visa and Mastercard, alleging fees restricted competition in breach of EU law proves that the market needs to change.

This is a critical turning point for the global payments industry, not just the UK's. In August, the Canadian finance minister announced new commitments from Visa, Mastercard and American Express to lower costs for small and medium-sized businesses. With lower interchange fees, businesses can save money and invest back in to the business to support growth – and ultimately, pass the savings on to consumers. In the same month, the Australian Productivity Commission published a report reviewing the balance between competition and stability in banking, due to market dominance of the big four banks in Australia, and called for interchange fees to be eliminated.

## How a single market can transform the industry

Just as price comparison sites have done for consumers, a single marketplace takes an intricate world and streamlines it into one clear and simple platform which is easy to navigate. Merchants can see how costs compare, get expert advice on payment providers that will best suit their needs, reduce costs of payments acceptance and in turn increase sales by passing down lower costs onto their customers.

This creates opportunities for beneficial relationships between acquirers, payment providers and merchants. New and innovative payment providers benefit from greater exposure in a market currently dominated by big industry players, giving them access to new business leads in a market where new customers are hard to come by. In turn, merchants benefit from improved prices and services as a result of greater competition.

In the single marketplace, merchants can save upwards of 15% on fees – in a rapidly expanding industry where digital payments are expected to hit 726 billion by 2020, the savings potential is enormous. With consumers embracing the convenience of plastic more and more, the APEXX marketplace will introduce much needed transparency, efficiency and competition into the market.



Peter Keenan, CEO, APEXX



# Cognizant

**Abhijit Deb,**

Head of Banking & Financial Services,  
UK & Ireland, Cognizant

Abhijit Deb is the Head of Banking & Financial Services in the UK and Ireland for global professional services and technology consultancy Cognizant, helping clients in the financial sector develop their digital transformation strategies.





# INNOVATION AND COMMODITISATION: EXTRACTING VALUE FROM THE NEW ERA OF PAYMENTS

Consumers now expect easy and immediate payment services, no matter where they are or what they are buying, whatever the payment method. It may be symptomatic of the 'age of instant gratification,' but it also demonstrates how people value financial agility. This was highlighted by a recent system failure with the UK's Faster Payments System that caused mass inconvenience and frustration among consumers. Whether paying a friend back for last night's dinner or sending emergency funds to family travelling overseas, the offerings of digital banks such as Monzo and Starling are testament to the industry's efforts to keep up with rapidly evolving consumer expectations. This trend has now also filtered into the business world.

As global business and cross-border transactions have proliferated, there are significant implications for commercial customers who rely on banks and payments providers to provide a flawless service faster than ever. The technological saturation of the financial services industry has been met with an increasing affinity for risk amongst business customers. Churn has never been easier. If one bank cannot meet their needs, customers can leave, and it has never been easier for them to switch financial providers in a congested market. In essence, the evolution of the payments ecosystem encompasses much more than innovation targeted at consumers.

## Understanding the value of payment data

Of course, there are some interesting examples of innovation in consumer payments. Gemalto's biometric bank card, for example, highlights that the area is steadily advancing, despite scepticism that there will be mass consumer acceptance.

However, the pace of change is accelerating rapidly in terms of offerings.

For instance, blockchain is being harnessed by banks and technology vendors as a prime enabler of an instant B2B payments infrastructure. Industry players realise that the methods that can derive benefits today are largely based on a better understanding of the value of payment data.

While such data has mostly been used to create a hyper-personalised customer experience for consumers, it is increasingly being harnessed in services to businesses, even outside the financial services sector with companies such as Google recently purchasing Mastercard credit card information to track users' spending to create an additional revenue stream.

This evolution of B2B product consumption is emerging as a key theme across the broader financial services market and is increasingly allowing businesses of all sizes to 'window shop' for the products and services they want the most. Providers are racing to commercialise the increasing amounts of account information, a trend that has increased in the wake of regulation such as PSD2 (the Second Payment Services Directive). By doing so, they can position themselves as the customer's 'digital front door' to a wider range of services such as financial advice, merging the dimensions of 'fast money' (a consumer's daily spending) and 'slow money' (future spending, saving and investment).

Adopting innovations such as automation, means that banks and card providers can help their commercial customers transform payments into a process that can add real value and allow the integration of additional services. By making financial reporting much easier, organisations can glean better insights into data showing purchasing trends among their customer base. The emergence of machine learning and self-learning systems will make this process much more efficient,

even incorporating features like automated financial advice or fraud detection to become commonplace.

## Consumption models are changing

Therefore, as payments processors and providers realise the opportunities in the business payments ecosystem, innovation accompanied by a commoditisation of payments services is on the increase, characterised by providers trying to add more value in the supply chain. Although currently most relevant to the SME market, companies of all sizes are being targeted with added value payments services such as reporting, to help them make better decisions. For example, retailers working with Barclays have access to add-ons and third party apps via the bank's SmartBusiness Dashboard, including basic analytics to see what customers are spending their money on. This information can then inform marketing schemes that tailor product promotions to specific customers.

Ultimately, the more choice the customer has and the more informed they feel, the more likely they are to return to the same bank to take out a loan or use other services.

With so many contributors to the payments ecosystem, and an increasing number of organisations using the analysis of payment data as a key differentiator against competitors, it is crucial that banks, regulators and payments processors co-ordinate their efforts and use the best technology available to create an efficient system. And with the Faster Payments Service deal up for renewal, a system that underpins most of the UK's banks and building societies, perhaps it is time for the government to consider how it can best support a payments infrastructure that works for all.



Written by Patrick Kleuters,  
SVP Europe, Gemalto

# ENSURING BANKS TAKE THE RIGHT APPROACH TO DIGITAL ID SCHEMES

Proving your digital identity is very much a 21st century problem. For the first generation of internet users, proving you were who you say you were wasn't an issue. They just needed to trust the website and the information it was providing, not the other way around. Today however, companies are recognising that if they don't provide an online service, they will fall behind. They need a digital offering to stay competitive. And now, we're experiencing a boom in online services which require ID authentication – from signing up to a new mobile service to renting a holiday home.

The issue is that in the absence of any properly designed, ubiquitous identification frameworks, many services have evolved independently, leading to inconsistent and limited solutions. The quality of the customer experience has in fact fallen, leading to distrust and apathy towards identity schemes.

Fortunately, banks are well placed to fix this internet identity crisis. PSD2 requires banks to support Strong Customer Authentication for all their customers, which means radically revisiting their approaches to fraud prevention and how they identify customers. In fact, the regulation gives banks the perfect excuse to work together to fix the usability and

convenience problems posed by current online authentication schemes. By controlling the identity verification process and becoming identity and data protection providers, banks could deploy the solutions that become the de facto standard for securing the internet.

But first, banks must make sure they are taking the correct approach to be successful. Below are some key considerations to ensure successful deployment.

## Building trust

First and foremost, banks must address issues of trust. The modern, digital world has made society distrustful of third parties and the handling of data. It is the confidence the customer has in the controller of their data that will determine the uptake, and success, of any digital identity scheme. Currently, banks have two primary models to choose from and they must decide which is right for them and their customer base.

A Federated Identity approach would see the customer relinquish primary control of their data to a trusted provider, normally the bank. For banks, this streamlines the entire process, allowing them to validate the authenticity of the individual's identity

when they enrol for a new service, and then become the focal point of trust for other services and providers. Under this approach, customers can reuse credentials for multiple services. They simply log in on one website and then access others without having to create another profile or type another username and password each time. It works because the other sites trust that the identity provider (in this case, the bank) has authenticated the user to a certain standard and so they permit access.

More recently however, another type of model has emerged, which is more decentralised and based on evolving technology such as Blockchain. This model places the end user fully in control and allows different service providers to share identity verifications. This is called the Self Sovereign Identities model. With this approach, service providers can simplify customer identity management and streamline the due diligence process while enabling end users to be in total control of their identity. Users only share what they must and can prevent third-parties from registering their data. The best-known example of a successful SSI scheme is Sovrin in the US, which is working with IBM and T-Lab to provide a decentralised global identity scheme.

## Never forget privacy

It's not just trust which banks must get right. Privacy remains a key driver of the user experience and will be crucial in onboarding customers. In any identity model, clear boundaries to limit the visibility of personal data to each participant will be important. To work with this, banks can temper the 'blinding' to limit the degree to which each participant is aware of the user's actions and their data. Adopting a non-blinded model would mean that the user's information is exchanged between the identity provider and the third party, usually with or without the customer's knowledge. It's commonly used to enable individuals to access websites using their Google or Facebook logins. In this situation, the customer is redirected to login into their account before they can access the service.

A blinded model, on the other hand, would ensure that no personal data is exchanged between either party. To achieve this, all claims are sent through a central, independent hub which acts as a buffer between the identity provider and the third party. While this boosts the user's privacy, it does not encrypt any data, instead relying on the trusted hub to securely handle and process before passing onto either party.

Banks must decide which aligns closely with the needs of their customer base.

## Collaboration breeds success

Over the last year, we have seen several bank-driven initiatives in the digital identity space. For example, in Canada, Bank of Montreal, Canadian Imperial Bank of Commerce, Desjardins Group, Royal Bank of Canada, Scotiabank and TD Bank have made significant strides in implementing identity solutions through blockchain. These have been designed to allow customers to use an app to verify their identity and only show the service provider what it needs to see, with all other personal information remaining private.

Similarly, in the UK, customers registered for Barclays online banking can now use this log-on as part of the UK Government's GOV.UK Verify registration process, which helps customers by pre-filling forms and negating the need to repeat ID authentication processes.

Such collaboration is vital for the success of digital identity schemes in the



future. Not only will these models fail if most banks refuse to get involved, but collaboration – whether it's government or banking led – vastly improves the possible use cases and services, bringing greater customer satisfaction and engagement. Collaboration also will help lead to standardization, and through using one model rather than several different ones, it's more likely to reach a critical mass for other services and industries. Take Bank ID in Sweden, for example, which was a result of several banks collaborating on one identity scheme. It now reaches 6.5 million internet customers who have the option to use it with more than 300 different service applications.

## Fulfilling the potential

For a ubiquitous digital identity scheme to be successful, banks must have the vision and strategy in place to drive change. Developments in Europe show that it can be done, if banks take an active and engaged role. With the likes of card payments, faster payments and SEPA, banks have a long history of collaboration to create an ecosystem that delivers value to all participants. Now is the time for banks to come together and realise the opportunity that is in front of them. Collaborate and align their digital ID schemes with the needs of their customers and their approach could very quickly become pan-European or set the precedent for how people verify their identity across the entire internet.


## About Patrick Kleuters

Patrick Kleuters has been SVP for Banking and Payment since early 2017. In his role, he is managing and developing the complementary and integrated digital arm of the banking and payment offering with clients. He is helping banks and other financial institutions to reap the benefits of the mounting regulations across Europe – with a particular interest and focus on digital identity solutions and schemes.

Patrick has more than 15 years of demonstrated history of working in the IT industry and in various team leading & sales positions. He is skilled in building trusted relationships and represent a track record around security and innovation of identity solutions in telecoms, banking and payment related services.

Patrick graduated in International Business from the University of Maastricht and later he spent his Erasmus years in Cambridge and Barcelona. Fluent in 5 European languages; he positions as a bridge builder between various cultures.



A professional portrait of a middle-aged man with short, graying hair, wearing glasses, a dark suit jacket, a light blue shirt, and a blue patterned tie. He is looking directly at the camera with a slight smile. The background is a plain, light-colored wall.

**Rahul Singh,**  
President of Financial Services,  
HCL

**TECH HOLDS  
THE KEY:  
HOW FINANCIAL  
SERVICES  
ESTABLISHMENTS  
CAN FIGHT OFF  
THE FINTECH  
THREAT**

For all the talk of FinTech disruption, it's interesting that the banking industry still widely uses 60-year-old computer language COBOL. It powers 95 per cent of ATMs and 80 per cent of in-person transactions, with one recent estimate suggesting that there are 220 billion lines of COBOL code currently run across banks. This raises significant questions that must be addressed if financial institutions want to keep up with their competitors: can COBOL really drive innovation? Can it target young programmers who are attracted by the prospect of using systems like Python, Java, Erlang and Scala? It is the likes of large corporate organisations such as Google and Apple which allow young talent to play with these programming languages, making this an issue finance professionals cannot afford to ignore.

The reality is that financial institutions must get their tools and techniques right if they are going to compete with FinTechs. You don't have to look far to see examples of companies offering more to consumers and businesses alike: take Robinhood's offer of trading without charging a commission, Prosper's connection between borrowers and investors for unsecured personal loans, and SoFi's offer of student loan refinancing. Even FinTechs which were once considered upstarts are increasingly dominating the financial services space. Paytm, for instance, didn't exist until eight years ago, yet manages mobile payments for 300 million registered users. Likewise, Alibaba's Yuebao is one of the largest money market funds, yet only launched in 2013. One thing is clear: regardless of their time on the scene, FinTechs are driving the future of the financial services industry.

One big advantage FinTechs have, by their very nature, is a lack of legacy technology. The story is very different for the wider industry: a recent survey from HCL Technologies revealed that almost two thirds (60 per cent) of financial institutions cite legacy applications as their biggest barrier to agility, innovation and disruption. Typically, traditional financial services organisations are tasked with managing these burdensome outdated applications, which restrict the adoption of new technology. FinTechs, by contrast, especially the more recently-founded companies like those listed above, have no such problem. Without the weight of obsolete legacy systems on their shoulders, they are better positioned to maximise the potential of new technology. The challenge,

then, for traditional players in the financial services game, is simply to stay abreast. When FinTechs already have a head start, the need for financial institutions to up their game and embrace digital transformation becomes even more pivotal. Losing pace with the competition is simply not an option.

## Biting the technology bullet

To put the scale at which new technology is being used into perspective, global investments in FinTech were estimated to be \$31 billion in 2017. That level of investment has the potential to drive serious change in the world of financial services. This leaves one path for traditional service providers who have the painful task of adapting to the coming challenges: to relentlessly examine trends and identify technologies that can catapult them into the future.

Trends are relatively easy to identify, even though consumer behaviour is rapidly changing; the problem lies in responding to the trends. The world of financial services is bristling with regulatory and compliance restrictions, meaning enforcing change can be painfully slow. Worryingly, even financial institutions in the Fortune 500 are fighting to keep pace. These institutions must recognise that technology is driving change in the finance industry, and that investments in technology will help re-shape processes, products and business models quickly and cost-effectively. In other words, technology will keep financial services organisations agile. Embracing technological innovation is the only solution these institutions can use to respond to changing trends and keep risk under check.

Simple approaches to a complex problem. Identifying the issue, however, is only half the answer. It is crucial for ambitious financial services CIOs to consider which technologies they should be directing their attention towards. In the maze of new technologies dominating the industry, where should the organisation place its bets? The financial space is becoming increasingly dominated by cloud, mobile, automation, big data, analytics, artificial intelligence, natural language processing, cybersecurity and blockchain. Each in itself is a powerful driver of change, making it difficult for a CIO to pilot an organisation around these options.

The first step is to understand the future of financial services and the direction in which an organisation needs to innovate. It then needs to identify the technology (or combination of technologies) that will move it faster in the chosen direction and simultaneously help reach momentum within the industry.

It sounds simple on paper, but how can this change be delivered in practice? There are two strategic aspects to keep in mind:

- A distinct long-term technology roadmap must be developed separately from short term goals. The long-term roadmap should leverage a range of technologies rather than a single overarching one. When combined, these technologies deliver more than the sum of their parts, considerably elevating the quality of the customer's end experience.
- Relentless experimentation is key. Only by testing out these technologies will financial services institutions be able to understand which must be adopted to improve the pace of innovation and meet business goals. Ideally, these organisations should venture out and partner with smaller boutique firms, too, since partnerships like these often result in unconventional but highly effective solutions. If financial services organisations want to remain on the path to agility and compete with market leaders, they must be willing to branch out beyond their comfort zone and embrace change.

## Innovation is key

By ensuring innovation is driven by a sharp strategic focus and powerful technological partnerships, financial services organisations can address the challenges posed by legacy applications. The problem facing these institutions may seem complex, but the solution is surprisingly straightforward. To avoid further domination of the financial services space by increasingly powerful FinTechs, traditional organisations should refrain from putting their eggs in one basket and instead experiment with emerging technologies, all the while creating a diverse and innovative long-term strategy. Only by following these steps can financial services institutions keep up with the competition and stay ahead of the ever-changing game.



Steven Murdoch,  
Innovation Security Architect,  
OneSpan

# UNDERSTANDING THE FACES OF BANKING FRAUD — IMPROVING DETECTION AND PREVENTION IN AN EVOLVING THREAT LANDSCAPE

Fraud isn't a new phenomenon in banking and financial institutions, but with the rise in mobile and digital banking, the nature of fraud is changing. We're seeing an increase in the sophistication of banking fraud techniques, and attacks are evolving at staggering rates across channels. Yet, while security awareness and budgets are on the rise, a recent report found that only 38 per cent of banking and security leaders have high confidence in their organisation's ability to detect and prevent fraud. Logically, banking fraud should reduce as security budgets and awareness increases but evidently this isn't the reality. Therefore, to ensure that banks and their customers are as safe as possible, it's important to have a thorough understanding of the threats faced by banks, as well as the steps they can take to mitigate them.

## Banks must understand the threat landscape

To get a handle on the issue of fraud banks need to, first of all, understand the regional disparity in the most common types of fraud. For example, online payments are far more common in Europe which means phishing presents a more significant threat than in regions where check payments dominate. European banks face the challenge of securely establishing what transaction the customer wants to perform, despite attacks targeting communication between banks and their customers. Strong customer authentication, as required by the EU Payment Services Directive 2, can help here by not only verifying who the customer is, but also ensuring that the customer is aware of the transaction taking place. While this can boost security and

customer authentication, it doesn't provide a fool-proof solution against phishing.

## Banks must keep an eye on cross-channel vulnerabilities

In the same way that different regions present different challenges, the channels used for banking also hold their own unique difficulties. For example, banking in-person may be inconvenient, but it's going to be harder to pretend to be someone you're not, or con someone face to face. That isn't to say that in-person banking is necessarily safer than online or mobile banking, but that different channels will face different threats.

The mobile channel also has its own challenges, including poor software updating practices by hardware vendors. While regulators need to take action to improve the provision of software updates, for now banks will have to assume that there'll be unpatched flaws and design fraud prevention measures to accommodate and mitigate this risk.

Online banking faces similar challenges as mobile banking but with the added difficulty that applications are generally not protected from each other and there are no app-store enforced restrictions over what software customers can install on their computer.

While different channels offer their own unique challenges, there are also similarities in how they're addressed. For example, multi-factor authentication as a method of enhancing security can be found on both mobile and online banking.





## So why isn't banking fraud reducing despite increasing security budgets?

Even though money is being pumped into cyber security, many banking and security leaders continue to see steady or rising fraud levels. There are two main reasons for this.

Firstly, criminals are adapting to existing security measures and improving their attacks. They're doing this by trading knowledge through underground marketplaces that allow criminals to specialise in particular aspects of fraud. This could be anything from breaking into accounts, money laundering, or obtaining security credentials. By sharing knowledge, tips and hacks with each other they're able to stay one step ahead of security measures.

The second reason is a consequence of the goal of some security initiatives. Instead of trying to reduce overall levels of fraud, banks are applying security techniques that facilitate new business opportunities while keeping fraud under control.

## What can be done to improve fraud detection and prevention?

Given that customers are often both the main target for many types of fraud, it's helpful they have an understanding of the threats they face. Unfortunately, customer education in banking is generally ineffective at reducing fraud because customers are focussed on carrying out the transaction, rather than on security. Each bank also has different rules and procedures and these change over time, so customers

are easily confused as to what the bank expects them to do. Security technology should therefore be designed to work for customers, without imposing a burden on their time and attention, and taking into account the context in which transactions are performed.

Banks must also focus on improving employee confidence and providing a frictionless customer experience. It's a problem that only 38 per cent of respondents to a recent survey had high confidence in their organisation's ability to detect and prevent fraud before it causes serious damage. This sentiment speaks to the increase in fraud incidents and losses, and it accounts for organisations' inability to detect and respond to fraud incidents in anything close to real time. The message is clear: traditional anti-fraud controls are not sufficient for stopping today's determined fraud efforts.

As the banking experience transitions more from the branch and the laptop to the mobile device, institutions need to be increasingly mindful of their customers' expectations of user experience and ensure that customers can do business through convenient channels. Achieving this requires deployment of authentication and transaction controls that are both effective and efficient.

Banking customers have more options than ever before, and if your security controls are perceived as a barrier to customers conducting transactions, then they will either try to bypass security controls or take their custom to another institution. Those banking institutions that can deliver a convenient and secure user experience will likely win more customers, sell more services and suffer fewer losses.

2018 has been a huge year for partnerships across the payments industry. In particular, we've seen collaboration between the retail and payments industries, with e-commerce giants like Walmart partnering with payments titans like PayPal, and the newer market players like Venmo handling up to \$12 billion in transactions in the first quarter alone. These partnerships have one common goal: to fight for a bigger share of the wallet.

To form the most successful partnerships though, companies must approach with a rational and considered mindset, starting by identifying the key players that they need to collaborate with. The most profitable partnerships will recognise and capitalise on each other's strengths to deliver industry leading market offerings.

In the case of strong retail and payment partnerships, the benefits are clear. Retailers can meet customer expectation by delivering a seamless payment process and the payment service provider increases transactions and gains better access to a global network of engaged consumers.

## The changing face of retail

The retail industry is in the midst of a revolution. The widespread global adoption of online devices means that technology is permeating every aspect of the shopping experience, creating a host of challenges and opportunities for consumers and merchants alike.

Data collected from those online devices is used by retailers to tailor their respective shopping experience, from the very first targeted ad, to the payment transaction and delivery method. When considering that, according to PwC's 2018 Global Consumer Insights Survey, social networks ranked number one for finding inspiration for purchases, it is fair to say that consumer experience and the projection of a company's online brand has never been so important. If businesses are to succeed in the digital era, leaders must ensure that their consumer offering is of a consistently high quality, globally competitive and as hassle free as possible. Adobe's eConsultancy Study shows that merchants recognise this, with 54% of retailers considering customer experience to be their most important focus.

## The importance of collaborative partnerships for scalability

One fundamental pillar that is integral to positive customer experience, and consequently merchant success, is the payment infrastructure. Consumers have become accustomed to an 'always-on' lifestyle where connectivity and convenience are no longer considered luxuries, but essentials. This 'always-on' attitude manifests itself in the retail sector through the expectation for instantaneous service and transactions. This is especially prominent in the e-commerce sector where consumers are able to access services at any time on their smartphone, expecting the same quality of service every time they do.

The e-commerce market is not one that merchants can afford to ignore. Statista's research shows that in 2017, retail e-commerce sales worldwide amounted to 2.3 trillion US dollars and e-retail revenues are projected to grow to 4.88 trillion US dollars in 2021. Merchants need a payment infrastructure that is capable of scaling in line with this rapid growth and are increasingly turning to more deeply integrated partnerships with payment providers to ensure they deliver the speed that consumers are looking for.

Astute leadership teams will forge partnerships that place technological innovation at the very heart of a combined business

model, allowing them to become market leaders through a combination of reputation built on heritage and new business models that fully capitalise on the benefits of technology.

## The consumer benefits

Partnerships between retailers and payment service providers can have huge benefits to the end user. Firstly, and perhaps most noticeably, will be an improved user experience. More sophisticated and modern payment infrastructure will contribute to a fast, frictionless transaction experience. Better connectivity will make international payments seamless.

Secondly, as payment service providers are duty bound to adhere to stringent regulation around data safeguarding, a consistently high quality of security is guaranteed. This leaves the consumer safe in the knowledge that their personal payment details are well protected against fraud and breaches.

Lastly, by partnering with a global payment service provider, it is likely that retailers will be able to offer international consumers a payment method tailored to their local market. By offering this level of interoperability between global transactions and local market nuances, retailers will capture the entire market potential. For example, in Brazil as much as 70% of local payments are made by card payments with instalments and almost a quarter of online payments are made with Boleto Bancario, a cash payment method. If they fail to offer local payment processes, merchants could miss out on significant opportunities to increase revenue.

## Creating walled gardens

While the impact of these partnerships is predominantly positive for consumers, as with any innovation or large partnerships, we must not overlook potential downsides. Online devices are generating more and more data that retailers can use to hyper-personalise product offering. As retailers and other large platforms expand to offer a huge range of products and services, allowing customers to consume, buy or enjoy almost anything, there is a real danger that we see the creation of a walled garden.

These all-encompassing retail models only work if they can capture a majority share of the consumer's time, money and attention. It is easy to predict that partnerships will become more exclusive, providing certain services only to a specific platform or retailer in order to differentiate themselves from the competition. This may ultimately limit consumer choice, compared to a fully open and interoperable internet.

## The future

It's clear to see that partnerships between retailers or platforms and payment service providers will become an increasingly prevalent trend across the payment landscape. In particular, we are likely to see smaller, more technologically innovative players being acquired and used by their partners to get ahead in the increasingly competitive market landscape.

Partnerships can be unpredictable and challenging, but one thing is for certain, they hold unparalleled opportunity for innovation. Even more so than in 2018, we can expect to see partnerships being formed in 2019 that are bigger, more exclusive and of a higher investment value.





**Matthias Setzer,**  
CCO, PayU

Matthias joined PayU as the Chief Commercial Officer in October 2016. In this role he is responsible for PayU's cross-border business, global sales, key accounts, strategic partnerships and marketing & PR. Before joining PayU, he worked with PayPal for over 12 years in various roles, most recently as their Senior Director Strategic Partnerships & Biz Development EMEA, based in Luxembourg.

Matthias holds a Masters degree from WHU in Vallendar, Germany.

# THE FUTURE OF PAYMENT PARTNERSHIPS





# THE SECRET TO REDUCING TRANSACTION ABANDONMENT: BEHAVIORAL BIOMETRICS

Few markets face as much fierce competition as eCommerce. With giants like eBay, Amazon, and Walmart dominating the industry, companies need to differentiate themselves in ways that will not only attract customers but encourage them to buy more. Establishing customer trust and loyalty, creating a flawless user experience, fast online storefronts, and rapidly adopting new technologies are all a given necessity, not a choice.

One of the challenges online retailers face is transaction abandonment. 53% of customers abandoned a transaction in 2018, resulting in lost revenue in the billions for retailers. With so much at stake, it's vital that online merchants make

their shopping experiences as easy and as engaging as possible.

## So Close and Yet So Far: Losses Due to Transaction Abandonment

Abandoned transactions carry huge amounts of lost potential profit. 20–30% of eCommerce customers abandon the checkout process during the payment phase, even after providing personal and delivery information. For 36% of online retailers, at least 40% of mobile payments are abandoned during checkout. While the reasons for abandonment vary, nearly two-thirds of shoppers cited having to remember

authentication details, like passwords, as the primary reason.

## Online Payment Friction Points

Payment is a double-edged sword in eCommerce. On the one hand, customers need a variety of ways to pay for products securely. On the other hand, each payment method involves an intricate dance between your eCommerce platform, payment processors, credit/debit card vendors, and banks. Let's not forget about compliance regulations that dictate the level of authentication needed. During this dance, customers are often asked to authenticate themselves multiple times. Each of these hurdles causes a break in the customer's

**Noa Benari,**  
VP Marketing,  
SecuredTouch

Noa has a track record of success in building emerging technology companies into category leaders. Prior to SecuredTouch, Noa was among CyberArk's (NASDAQ: CYBR) earliest employees, where she held various senior marketing roles in EMEA and Asia Pacific, supporting the company's global marketing strategy through its initial public offering in 2014.

Poor experiences like this contribute significantly to transaction abandonment. Without even factoring in the customer's mood after the process, this negative experience influences a customer's decision whether or not to revisit this website.

## Passive Authentication – Reducing eCommerce Transaction Abandonment

Sharon Manikon, Managing Director of Customer Solutions at Barclaycard, emphasizes the importance of embracing new technologies: "Payment technology is continuing to evolve at pace and...small businesses who don't keep up with this rate of change are potentially missing out on both sales and customers."

Reducing friction means using an authentication method that doesn't require customers to jump over multiple hurdles. Making transactions as easy as possible can drastically reduce the abandonment rate. Fingerprints and facial recognition scans are a good start (AKA static biometrics), but merchants need to go one step further.

The chosen solutions must take securing against fraud into account. Cybercriminals have developed sophisticated methods of bypassing traditional fraud detection methods such as device fingerprinting and rule-based detection. Account takeover (ATO) fraud alone cost merchants and consumers \$5.1 billion in 2017. In addition to offering a smoother experience, merchants need authentication solutions that aren't vulnerable to theft or copying.

For this reason, more apps are recognizing the value of behavioral biometric authentication, providing high levels of security while reducing friction and working seamlessly in the background. For customers, it's a no-brainer: instead of remembering dozens of passwords, simple combinations of a few gestures (a swipe, a tap, etc.) provide sufficient data to authenticate themselves. Furthermore, they do not need to provide any personally identifiable information, so they are more likely to want to complete the payment. The result is faster and safer transactions for both customers and merchants.

purchase flow and is an incentive to leave the transaction for something easier.

Specifically, for mobile users, the process is (a) more frustrating and (b) vulnerable to more attack vectors. The payment process often bounces customers to different sites that are not optimized for mobile, slow to load, require some form of step-up authentication, require them to open an account or use a password (one of many) that the customer doesn't remember. Through no fault of the service provider, the customer gets too frustrated to follow through with the order.

### Friction Point Walk-Through

To illustrate this problem, imagine Tim is placing a typical online order.

#### Friction Points

1. When Tim clicks 'Pay Now,' he needs to authenticate himself. Many websites let users save their billing and shipping information, which usually means remembering a username and password.
2. Tim enters his payment details and is redirected to a payment gateway, which verifies his payment info. This might require more information, often personal data, that Tim needs to remember – creating delays.
3. Tim is redirected back to the service provider page where he is asked to confirm whether he wants to make this payment.
4. If any errors occur or if authentication fails, Tim may need to authenticate again.



**SECUREDTOUCH**



**Richard Price,**  
Head of Financial Services  
Practice – UK&I,  
TIBCO







# TRANSFORMING THE INSURANCE CUSTOMER JOURNEY WITH AI

Like players in any highly competitive service industry, insurers need to find ways to improve the experience of their customers as part of sustaining loyalty and, ultimately, developing and enriching the customer journey.

Insurance firms face difficulties here that are not shared by all in the broader financial services community. They may well enjoy just the one brief touchpoint per customer per year, at premium renewal time, and so must make the most of that limited opportunity not only to cement the relationship but to explore the possibility of selling additional services.

However, by deploying the right AI strategy, insurers can transform customer relationships for the better, while helping to streamline their own operations and boost profitability.

## Understanding customers

The insurance industry lags behind a number of other verticals in its use of AI to enhance the customer journey. An industry that can, at times, be conservative and traditionally-minded must overcome the nervousness that deployment of AI can provoke and try to learn from the gains made in verticals like retail banking, capital markets and telco.

Insurers may be somewhat unfamiliar with AI, but they are not blind to the urgent need to understand their customers better than they do now, and to develop a more personal relationship with them in order that their offer can be more tailored. They need a means of empowering the customer-facing employee by putting all necessary information at their fingertips.

Insurers are challenged to find ways to achieve greater granularity around the profiling of customers, as well as a much more detailed understanding of associated risk, judged on a customer by customer basis.

Visibility is a critical element in the understanding of both the customer and how insurance companies interact with them at all stages in the customer journey. Traditionally, internal views of the customer are based on historical reporting, founded upon fixed ideas on how to measure success or failure. The pace of business

is accelerating relentlessly, this brings the need for insurance companies to provide more timely, customised and interactive windows into the business. No longer is it sufficient to know what happened last week or month; different roles within an organisation need to see immediately when things are going wrong and be given the tools to understand why and react accordingly. Advanced analytics and AI can provide this awareness and insight across the business.

Insurers of all kinds must do better with the quote process, and learn to make better use of the customer touchpoints they have. They must furthermore look at ways to automate some of the more basic dealings they have with customers in order to free more resources to manage the higher end of the customer base.

Insurers are also challenged by the need to, at all points, remain transparent to the regulator. It is from here that much of their nervousness stems, and with good reason. To a regulator, 'customer innovation' or 'optimisation of the customer journey' can sound like attempted exploitation. How can they maintain transparency to the regulator while building intimacy with the customer? Where is the solution that delivers this?

## Finding the right AI

Insurers can start to resolve these challenges with the help of AI. But rather than adopt just any AI-based solution, they must look for one that works for their type of business. An appropriate AI model that draws on the right datasets as the basis for advanced analytics should be their goal.

With the right AI model, insurers can look forward to creating efficiencies in their business while opening up new revenue possibilities. Risk can be better assessed, and claims processed more effectively.

Today's powerful and scalable AI platforms enable the implementation of advanced analytics and sophisticated models to better manage and extract value from the increasing amount of data pouring into an insurer's organisation. A platform like this is the basis of bespoke predictive models, machine-learning algorithms

and the consequent chance to optimise a multitude of business opportunities.

The use of augmented intelligence, for example, is a way for an insurer to judge where a potential new customer falls below the no offer line. At first sight, the prospect may appear to be just on the wrong side of the borderline between acceptable risk and too risky. But they might, with additional data, appear after all to be a good risk. If a client is clearly above the line, a good risk that is unlikely to claim, then clearly a similar level of intelligence is useful in deciding how to reward them so as to retain their loyalty.

AI can help to automate customer contact where appropriate, perhaps by enabling a sophisticated chatbot to guide the customer to a renewal or buying decision. Cross selling a customer from one line of insurance to another is clearly a great way to add incremental revenue, and AI can help here too. An AI platform can empower a employee in direct contact with a customer, helping them to cross sell to a car insurance customer by making them a disruptive home insurance offer during the brief renewal conversation.

But precision and care are needed to enable the customer-facing employee to make a pre-emptive offer that will be relevant and non-intrusive. Augmented intelligence is a crucial tool here, allowing the insurer to get closer to the risk model on the basis of knowing the customer better. It's about overlaying analysis on a standard insurance model to let you make the most of the short window where the customer has your attention. Without the right platform to deliver all the right information at the point of need, the moment is lost. It's about using AI to augment the human efforts of the employee by putting all relevant data on the customer in front of them at the critical time.

Augmented intelligence can transform the claims process too. A claim from a customer who has been with the insurer for 30 years and is known to be a low risk can be settled immediately. Another claim might require no more than an approval, with a second pair of eyes needed before it is resolved. A third category of claim involves assessment of potential fraud, or might just be a complex claim that needs to be referred to an assessor or the underwriter. Analytics can take about a third of this load off the insurer's hands, driving simple cases down a self-service route and delivering information to streamline the rest.

The basis of successfully deploying an AI platform lies in having access to relevant data and understanding it. With advanced analysis at their disposal, insurers can decide what processes they can automate and what regulator-friendly models they can build around AI.

The right model can personalise the customer journey and have a real and positive impact on customer relations. This level of personalisation can help both at premium renewal time and also at the potentially more stressful touchpoint of a claim being processed. It can help the insurer to present themselves as a trusted partner, able to go the extra yard with a response that is tailored to the individual customer.

By personalising the customer journey, AI can play a key part in minimising the threat of customer churn. It can be the basis of a more successful and meaningful way of keeping the customer on board than simply rewarding their loyalty with lower pricing. Indeed, finance-based loyalty incentives used indiscriminately can have the effect of making the customer feel they have previously been overcharged. Building trust and introducing a personal touch are arguably better weapons in the drive to keep hearts and minds.

## Adopting AI

The adoption of AI is not to be approached as a silver bullet, it needs to be seen as a journey towards a position where advanced analytics is at the heart of the business. Once established as the driving force in a transformed organisation, it must be seen as a journey of continuous measurement and improvement.

A measured approach to adoption will maintain stability and confidence internally and externally. The insurance market is dominated by the use of standard models that whilst providing stability and confidence, stifle competition. Foremost, in the traditional armoury is the venerable GLM, the bread and butter of the industry, well understood by all participants. Nervousness around the adoption of alternative tools means that the GLM is not going anywhere fast, but there is much that can be done to improve the way it is used. Selection and weighting of inputs into existing GLM models is a prime candidate for the use of advanced analytical techniques, bringing differentiation and innovation in a stepwise approach. Once the benefit of these new tools and techniques has been proven, the journey can continue. Evolution not revolution.

## Changing perceptions

Insurers are right to think that AI is not to be adopted lightly, but wrong to think that they can ignore it and get away with allowing competitors to get a head start on its deployment.

There are certainly issues and concerns that must be thought through. Many insurers, for example, are concerned that AI is all about replacing the human element of their business with machines, thereby stripping of them of a key asset. They must change their perceptions and learn to see that AI is about augmenting their employees, and that this is important for their business.

Other potential AI stumbling blocks include deploying it in such a way as to alienate customers, perhaps at the same time as putting insurers on the wrong side of the regulator. Properly used, AI will let the insurer retain the human touch that some of their customers expect, building on it through better availability of information on that customer.

Naturally some insurers will seek to use AI to automate some customer-facing processes. But even where AI is used to automate a process, there will always be customers who want the reassurance of a human to confirm an important detail for them before they finally click to buy. Many insurers will want to offer customers an AI-led self-service option as well as a lengthier human-led option, letting customers make the choice.

Ultimately AI will have multiple roles, helping to take some of the complexity and time out of customer management, letting some customers self-serve while supporting employees as they help customers with other more complex commercial decisions.

### From risk to opportunity

Used properly, AI can improve the customer interface, certainly when compared with existing models. Employees can be empowered and outcomes improved. Risk can be turned into a great opportunity.

Different insurers will use AI in different ways. Some may prioritise using it to mitigate fraud while for others it's more about better agility and responsiveness throughout their business. Others might deploy it as a tool to drive better premium values, or to cut response times from weeks to minutes. Nobody can afford to ignore it altogether. The future of customer relations, indeed of the whole business, may rest with it.

# OUT-THINK THE FUTURE OF BANKING AND FINANCIAL SERVICES



## WHY HCL?

### CULTURE



**ideapreneurship™**  
*Relationship™*  
 BEYOND THE CONTRACT

### INNOVATION



**MODE 1-2-3  
 STRATEGY**

### OUTCOME



**PARTNER OF CHOICE FOR  
 THE 21<sup>ST</sup> CENTURY ENTERPRISE**

For more details, contact [contact.fs@hcl.com](mailto:contact.fs@hcl.com)

WX8885



*Relationship™*  
 BEYOND THE CONTRACT

**HCL**

**Hello there! I am an Ideapreneur.** I believe that sustainable business outcomes are driven by relationships nurtured through values like trust, transparency and flexibility. I respect the contract, but believe in going beyond through collaboration, applied innovation and new generation partnership models that put your interest above everything else. Right now 119,000 Ideapreneurs are in a Relationship Beyond the Contract™ with 500 customers in 32 countries. **How can I help you?**



# ENSURING YOUR INSURANCE

Organisations in all sectors face increasingly virulent and sophisticated cyber threats – the insurance sector is no exception. The global insurance industry itself is estimated to be worth close to \$1 trillion annually, and whilst insurers provide protection to other firms, they themselves have become targets of data breaches and the risks they face are in a constant state of flux.

According to Accenture, a typical insurance organisation faces more than three effective attacks per month. In line with this, another report from EY found that almost half of insurers have seen “significant” cybersecurity incidents within their organisation.

## The Target

Cyber-risk can take many forms, from organised criminal groups seeking to obtain personally identifiable information (PII) and financial account data, to hackers trying to disrupt the day-to-day business of their targets, to APTs (advanced persistent threats) gathering intelligence and information to attack operations and customers.

The insurance industry has become a high-profile target, in part due to attackers moving away from the financial sector as they seek targets with a lower level of cybersecurity maturity. The sector continues to migrate towards digital channels to create closer customer relationships, driving highly-integrated platforms and portals, online application and claim enablement forms, as well as a whole gamut of app-based systems. As a result, the number of attack vectors available to cybercriminals has expanded and insurers, large and small, are now a long way behind the curve when it comes to shoring up their security infrastructure: the broader the attack surface, the bigger the window of opportunity for attackers.

Ultimately, managing cyber-risk is like managing your clients’ risk. It is not a binary of whether you get attacked, but a spectrum of how likely it is that an attack will happen. But, before the insurance industry can offer effective coverage to their customers, they must ensure that their own cybersecurity is up to the task. Worryingly, research from auditing firm KPMG found that only twenty percent of insurance CEOs believe that their firm is prepared for a cybersecurity event.

## Reality Check

With so few confident in their cyber defences, it’s hardly surprising that we have seen so many of data breaches in recent years. 2015 saw both Anthem (the second-largest health insurer in the US), and Premera Blue Cross suffer major breaches. Anthem had up to eighty million customer and employee records exfiltrated, and according to EY, the financial impact is expected to surpass Anthem’s own cybersecurity policy offered to its clients. In the same year, eleven million customers’ PII was stolen from Premera Blue Cross, which also had a hugely negative reputational and legal impact on the insurer. Unfortunately, attackers do not have to invest a great deal to breach an organisation, whereas insurers must allocate considerable resource to defend their assets. From a technical perspective, insurers are under constant pressure to modernise their infrastructure. However, this rush to innovate has its own pitfalls when it comes to managing cyber-risk, not least the increased emphasis on keeping critical data highly secure yet immediately available.

The nature of the data necessarily gathered by insurers is such that it is highly valuable to cybercriminals and this cannot be understated. It is one thing to store a username, password and credit card details. However, medical histories, financial situations and other extremely personal data is also collected, putting insurers at greater risk of attack.

To add to all this, insurance companies are placed under a huge amount of pressure to thwart these attacks whilst also meeting legislation – financial services and insurance organisations in particular are subject to a considerable amount of cybersecurity compliance regulation. The EU GDPR enforces that companies should “implement appropriate technical and organisational measures to ensure a level of security appropriate to risk”. Given that insurers have such a high level of risk, there is a significant onus on them to invest in cybersecurity tools and solutions to minimise the impact of cyberattacks on the enterprise that could affect their business and customers.

## Attacker Techniques

Cybercriminals leverage many techniques to penetrate corporate infrastructures and steal personal information and other valuable assets. Malware stealers are widely used by cybercriminals to acquire sensitive information, and trojans have multiple functionalities, such as man-in-the-browser techniques, keystroke logging, and form grabbing. Equally, Distributed Denial of Service (DDoS) attacks are a significant risk to insurers since their revenue will likely be disrupted as a direct result of an attack, and the repercussions in terms of costs for remediation and customer compensation are huge. Cryptominers are another attack vector that exploit unpatched known vulnerabilities, although this risk can be minimised by patching old servers and deploying relevant security measures.

Notably, ransomware is also a significant and growing risk to organisations across the globe, as multiple alerts of new and improved campaigns suggest. Insurers should be particularly cautious about ransomware given the highly competitive landscape of their marketplace and the importance of preserving their reputation.

With the need to outsource agreements, insurance companies specifically hand over control of important assets and data to third-party providers. Whilst this may bring business benefits, it also increases the risk of these assets being compromised, since the security protocols of the third-party suppliers may not be as robust as the protocols of the insurer themselves.

## The Solution

While cybersecurity strategies within the insurance sector are maturing, there are still many improvements that can be made. Ultimately it all comes down to making the right investments. Insurers need to try and stay one step ahead of their attackers. Investment efficiency, combined with an understanding of the importance of security from the top down, should drive the right allocation of funding. This can help prevent attacks, as well as mitigate their impact when one happens.

There is no single measure or technology that can achieve total prevention, so improving resilience on a continuous basis should be the overarching objective. Organisations need to put in place different complementary solutions to minimise the chance of suffering a data breach. Proactive threat monitoring technology helps to detect, in real time, external risks that have the potential to affect your organisation. Threat intelligence is actionable information, delivered in an automated way so that organisations can detect threats both inside and outside their network, and prioritise their responses. Proactive threat detection and monitoring through threat intelligence should be supplemented by a process of continuous cyber hygiene within the organisation.

Setting the appropriate alerts which detect intrusions can offer some protection, but an ongoing process of pen testing and patching is crucial for safeguarding the insurance company. The bad guys are constantly testing new ways to exploit your infrastructure, so remaining static when it comes to security protocols is a sure-fire way to get breached.

Performing periodic internal security reviews, red-teaming, and an ongoing process of education among all employees is critical. Cyber security is everybody's job – not just the remit of the IT team, and by establishing and promoting an appetite for cyber-risk management, insurers will find themselves better protected against enduring threats.



**Patryk Pilat,**  
Head of Pre-Sales Engineering at Blueliv.

The Blueliv logo, featuring the word "Blueliv" in a bold, dark blue sans-serif font. The letter "i" has a red dot, and the final "v" has a blue square at its base.

# TECHNOLOGY HAS NOT HELPED BUSINESSES SURVIVE – UNTIL NOW

Technology over the ages has made manual tasks easier and more effective, sometimes reducing speed, in many cases adding a level of accuracy that a human cannot achieve. The ethos of every step forward has been to produce benefit.

A clear example is the iPhone. There is no denying that it has had a fundamental impact on the way people across the globe interact, how businesses operate and crucially how processes are aggregated. Can you imagine carrying around a mobile phone, 300 CDs, your telephone book, diary and notepad? That's without the extras such as cameras, a stop watch, compass, the list goes on.

But, as technology has evolved, so too has the expectations of customers. As a result, businesses and banks are under pressure more than ever to embrace new capabilities and provide its customers with the streamline and seamless experience that is now the norm.

## The business disconnect

In many areas of our lives, technology has brought considerable benefits to the user.

However, in business we have experienced a flat line that is unaffected by technology. Despite two-thirds of businesses with employees surviving at their first two years, only 50 percent make it to the five-year mark and just one-third celebrate their 10-year anniversary. To put it simply, the rate that businesses are failing has changed only marginally in the last twenty years.

With pressure from across Europe to grow and technology opening a dynamic field of competition, there is clearly a disconnect. It can be argued that business owners have all the tools at their disposal to be successful, yet still the failure persists. The failure primarily is due to running out of cash.

## Cashflow is king

Cashflow is king in the business world. If you are not managing your cash you will face increasing issues and it will eventually result in closure.

So we should ask why has technology not solved this issue? Surely the solutions exist to resolve the problem. Well they do, the challenge is that they are complicated, often fragmented, and introduce a new complexity to business process

Businesses need simple, seamless and integrated solutions that provide visibility over their whole organisation. As entrepreneurs walk the fine line between success and failure, it is critical to get your revenue to exceed your costs. To do that you have to manage your cash.

## Managing cash and mitigating risk

The solution is not to treat cashflow management the same way as we handle accountancy or true financial tasks. They revolve traditionally around information from yesterday. What was spent, what was received, who has paid. No part of that focuses on the near future. The what happens tomorrow.

The Slide app has been designed with exactly that challenge in mind. Its goal is to place in front of the entrepreneur a different data set aggregated from others. Cashflow does not start at the reporting layer, it starts at the bank, so we started with a banking app. We know that the bank has many regular forecasted payments held in their records, so we wanted to make those clear

Furthermore, the biggest effect on cashflow will be the purchase ledger and sales ledger and we ensured that this was a key part of the aggregation within Slide. We then present that data to entrepreneurs in a simple way, categorising previous and future spend in the same way, so the yesterday, today and tomorrow are uniform. It makes the information usable, simple and familiar.

That is key, the issue in cashflow is that it has always been fragmented from the bank and other sources used. Businesses check their bank balance daily, we are allowing them to check their cashflow daily in the same solution. The user can see exactly when problems will arise not when they have, they get the greatest gift of all; time. They see the problems before they arise, and this allows businesses to forward plan, counter the problems by rescheduling payments and raising funding to get the best rates or to protect their cash at hand.

The challenge is that all accountancy systems and banks work in the past, the presentation of future view was always a separate task. We have aggregated that task and made it part of the today. We want businesses to succeed and reduce failure because of lack of cash visibility. We have focused on the yesterday, today and tomorrow leaving businesses with no more guesses.



**Simon Lyons,**  
Chief Commercial Officer,  
Slide



DoshEx

# DOSHEX: TOKENISING THE WORLD

This time Financial IT had a chance to interview Alex de Bruyn, CEO at DoshEx, a South African company pioneering the local development of crypto-tokens.

**Financial IT:** Hi Alex. Could you please introduce yourself and the DoshEx crypto-exchange?

**Alex:** Sure, I am Alex de Bruyn, the founder and CEO of DoshEx. I have spent the better half of the past decade navigating the banking space, and more specifically payments.

DoshEx is focused on building distributed business networks and tokenised solutions into day-to-day businesses. We build on both permissioned and public blockchains of varying degrees, based on the use case of the solution, to make sure it is fit-for-purpose at all times. This is all

linked back into our exchange to make it simple and convenient to exchange value between tokenised ecosystems.

**Financial IT:** What inspired you to launch DoshEx?

**Alex:** When I came across Bitcoin it intrigued me endlessly as perfect money.

The deeper and deeper I went down the rabbit hole, the more I was captivated by blockchain, crypto economics, and how it can truly solve some real world problems. I quickly realized that there were two camps in the blockchain space, those that are building new protocol layers and

coming up with the next best blockchain or cryptocurrency, and those that are building specific projects on blockchains trying to be the next big startup. We saw very few companies driving for adoption of blockchain and tokenization in our day-to-day businesses. So we decided to start focusing DoshEx at exactly that.

**Financial IT:** What is the core proposition that DoshEx offers?

**Alex:** Our core focus is the application of distributed networks and tokenization to our current business landscape to drive adoption of blockchain and crypto-economics.



**Financial IT:** *You have recently suggested that the impact of technology on emerging markets can be radically different to the impact on developed countries. Could you please elaborate?*

**Alex:** If we look at Bitcoin and blockchain, the media portrays it as technology designed to kill the first world banks and a group of cypherpunks that just want to stick it to the man. It may very well have started as that, however it has a much larger potential than just causing the downfall of the banking sector.

In African countries, it really has the ability to reach widespread financial inclusion. We can now, in a very simple fashion, transfer value to anyone anywhere in the world, which means anyone from the most rural places in the world can partake in our global economy. Something the banks haven't been able to achieve to date.

So, as developing countries, I believe we should pay close attention to this space, understand it and adopt the technologies that make sense, to leapfrog us into the next digital economy,

**Financial IT:** *Let's talk about South Africa in particular. What do you see as being the impact of cryptocurrencies?*

**Alex:** It really depends on what we define as cryptocurrencies. The development of micro crypto-tokens, will assist with the removal of cash from an ecosystem and make it more efficient to move value through a value chain.

By removing cash from our economy, it will help in the reduction of a lot of cash crimes that are prevalent in our society today.

Movement of money becomes immutable, which makes the identification of corruption and mismanagement of money easily auditable and traceable, which in turn will hopefully reduce it.

If we are looking at cryptocurrencies on a macro level, as in Bitcoin, Ethereum etc. It gives South Africans the opportunity to partake in a global economy effortlessly for the first time.

We can raise more capital, easier, to build local projects and businesses.

We can move value anywhere in the world effortlessly and allow for a hedge against the Rand when we see fit to do so.

For the first time, our location doesn't hinder us from creating or being exposed to opportunities globally.

**Financial IT:** *The last year or so have seen a speculative boom and bust in cryptocurrency markets. Trust and stability have been absent. What, in*

*your view, will take cryptocurrency markets to the next level of development?*

**Alex:** I think there are two main drivers that will stabilize cryptocurrencies. Adoption and utility. We need to move away from it being a speculative asset and start using it for its purpose.

For a currency to evolve into a medium of exchange, it needs to reach a certain level of adoption so that the opportunity cost of using it isn't higher than just holding it.

Once it reaches that level of adoption, the technology needs to be of such a nature that it is simple and easy to use in our day to day live.

We want to focus on building the base for the next generation of utility. By that we need to lay the foundation in our daily businesses to allow for the adoption in the market.

**Financial IT:** *Finally, where do you think that DoshEx will be in five years?*

**Alex:** I would like to see DoshEx as a trusted global brand for setting the standard as to how a distributed and tokenized future will look. With that I would like to have the strongest and most passionate core team in the space, focusing on realizing distributed technologies into day-to-day businesses.







# UNDERSTANDING THE CONTRACTUAL LANDSCAPE KEY TO PLOTTING THE 'BREXIT' ROUTE

Regardless of the 'type' of Brexit that is agreed, a shake-up of the way business and trade is conducted in the UK and across Europe, is a certainty. In the financial sector alone, bank contracts between the UK and EU are worth trillions of pounds. With the near limitless possibilities of change due to legal and regulatory consequences across such a large swathe of business activity, the contract repapering activity in almost any Brexit scenario could therefore be a colossal initiative. With the time limiting factor of a fixed transition period, it's vital that organisations begin the preparatory process in earnest.

Financial institutions large and small first need to closely analyse their business structures and contractual obligations to determine with whom they have contractual relationships, in which EU member state jurisdictions, the governing law, and whether and to what extent that relationship is currently impacted by EU legislation. This will enable them to understand the landscape within which they currently operate, determine how Brexit may impact their business and make informed decisions when attempting to mitigate the risk of post-Brexit disruption.

However, to determine which contracts may need to be repapered requires a far more detailed analysis of each individual contract. Even the most cursory consideration of the potential risks of Brexit would require an assessment of numerous factors: which obligations persist beyond Brexit; whether any

termination rights may be triggerable; whether a force majeure clause may be included and wide enough to potentially suspend performance of a contract; how customs or tariff changes may affect current business; and whether any products or areas of the business will be affected by loss of passporting. The list is endless.

Indeed, due to the scale of the contract repapering activity, financial institutions need to be well poised to take necessary action as soon as the legal consequences of Brexit become clear. As things stand today, successfully completing the contract repapering activity within a sensible timeframe, post Brexit, so that business isn't negatively impacted will be next to possible to achieve manually.

Only a technology-led approach through the application of artificial intelligence (AI) presents a realistic prospect of success. It is the only feasible approach to assessing and preparing for the multitude of contractual risks posed by Brexit. It will enable financial institutions to prepare for the new business environment and regulatory landscape that faces them.

## Digitisation of contracts

Perhaps the biggest obstacle for financial institutions today is a lack of visibility across their document universe. While wider digital transformation is underway in most financial institutions, few organisations have as yet digitised

their estate to an extent that supports analysis at a level of detail that can drive meaningful insight even across large volumes.

For instance, few firms are able to instantly identify derivatives contracts which contain Adverse Material Change clauses from across their document universe. Fewer firms still could instantly tell how many such agreements contain lifecycle events which will persist beyond 2019, and which may require authorisation following loss of passporting.

In the age of AI, the conversion of documents to electronic format is only the beginning of digitisation. The real value of digitisation is in providing organisations with the ability to query their document set at large volume and identify points of interest at a document level. It is this ability which firms need to cultivate in order to assess and prepare for the risks posed by Brexit.

## From Digitisation to discovery

In a digital contract landscape, quantifying the 'problem' becomes more achievable. Financial institutions can use a variety of data points to determine the scope of the repapering exercise. For instance, a logical search may be able to identify some contracts that terminate before 2019, or 2020 if such transition period is agreed. The organisation could then immediately disregard contracts terminating before 2020, focussing attention on those

continuing past this year. With contracts running conservatively into 100s of 1000s of documents, this can drive serious time savings against a wholly manual process.

However, the application of AI can deliver a deeper understanding of documents and drive even more sophisticated analysis. At a basic level, AI can go beyond simple logical search, and provide more accurate results for an analysis of 'simple' data points – such as termination date by examining individual contracts – utilising context and employing a greater understanding of the nature of the data point required. This approach can be extended to extraction of further data points such as termination clauses, and categorisation of such, to determine which contracts may have a right to terminate, if triggered by Brexit.

At the most advanced level, AI can answer some of the most complex questions posed by Brexit. For instance, following the loss of passporting, it is unlikely that existing contracts will simply be rendered illegal if they persist beyond the relevant date of exit. Instead, the question is more likely to be focused on whether firms can continue to provide new services (e.g. for 'lifecycle' events) required under existing obligations without obtaining relevant authorisation. Such an assessment, so called 'obligation extraction', can only be performed by human lawyers or the most sophisticated AI technologies. However, in the case of Brexit, it is only AI technologies that are able to achieve effective results in the short timeframe allowed to present any real solution.

Regardless of the form Brexit eventually takes, financial institutions will need to triage a vast volume of agreements to identify risks and prepare to quickly adapt to the new business environment through measures such as repapering, assignment, transfer or novation. Digitising and utilising AI techniques such as machine learning to understand contractual relationships is presently the only realistic way for financial institutions to understand the challenges they may face and adapt to what will be an evolving post-Brexit business environment. While organisations may adopt this approach immediately to deal with the Brexit challenge, the advantages of this approach will deliver long term business value and a capability that they will be able to apply to as yet unforeseen challenges in the future too.



**William Rees,**  
Business Consultant, iManage

William Rees has extensive experience of working in the legal services sector with expertise in equity research, corporate finance, investment banking and artificial intelligence. He is a qualified Barrister (2012 call) and door tenant at Civitas Law with interests in regulatory, commercial, construction and planning law.



Powering Islamic Financial Markets

# ISLAMIC FINANCE PRACTICES: LIMITATIONS AND PROHIBITIONS

In this short piece, I shall attempt to outline the main features of Islamic finance and Sharia-approved investments, as well as the categories of prohibitions and how they are related to Islamic values.

In practice, most Islamic financial institutions have established their own internal high-calibre board of religious scholars and advisors who examine carefully each financial transaction/investment to ensure its compliance with the Sharia.

The Sharia – literally meaning a clear path to be followed and observed – promotes first the principle of profit-loss sharing between financial institutions and entrepreneurs, thus emphasizing the spirit of cooperation in business which would help absorb the weight of loss when sharing it equitably.

From an Islamic perspective, the concept of asset-backing is prevalent, thus discouraging financial speculation as it

is not permissible in Islam. The Sharia law also encourages ethical, sustainable and environment-friendly finance while fostering financial inclusion. Hence, in line with the main aims of Islam for emphasizing on social welfare and supporting financial stability, these explicit in-built strengths form the backbone of the Islamic financial system, gaining an even greater appreciation on the distinct nature of Islamic finance.

These and other Sharia guidelines have shaped the types of financial transactions adopted by Islamic financial institutions. Accordingly, they have developed certain contracting models based on no-interest, risk-free concept to satisfy the needs of the market while covering major schools of thought.

## Practical Implications

A primary purpose for imposing these laws in Islam is to promote social justice





Rosie Kmeid  
Vice President, Global Corporate  
Communications & Marketing

Rosie brings to the post a wealth of experience in strategic positioning and campaigning having held various senior positions across a variety of sectors including audiovisual, IT and telecom, in addition to being the former Head of International Relations & Diplomacy at the Lebanese Presidential Palace. She is a regular speaker in international conferences and has over 30 publications in the area of Islamic finance with special focus on financial markets and IT trends. Rosie holds a Master's degree in International Law from the Université Panthéon-Assas (Paris II) and a BA in Political Sciences and International Affairs from the Lebanese American University. She has also attended various intensive programs at Harvard Business School and Cambridge Clare College, and speaks fluent French, English and Arabic.

and economic development. The Islamic code of conduct thus plays a vital role in keeping and nurturing the society in a harmonious state, while striving to make the world a better place to live in. In this context, Islam views the natural resources of the world and indeed human life itself, as a trust from Allah. Accordingly, as we move more and more into rapid development, these laws encourage believers to manage resources and opportunities effectively for future generations to come.

From a Sharia viewpoint, ethics dominates economics and not the other way around. Business ethics are an integral part of the Sharia which has certain foundation and principles on which the ethical values are based. Here the basic principles of business ethics may be characterized as follows: Fairness, integrity, dignity, loyalty and justice.

### Prohibitions in Islamic Finance

Islam is not only a religion, but also a complete way of life. In finance, Islam requires that all transactions be based on transparency, accuracy, and trust. In view of this, the Sharia has laid down rules in connection with Fiqh Al Muamalat which refers to financial or economic transactions within a general framework. As this is a rule based financial system, one must understand clearly what the fundamental rules are and how this system is different from others.

#### ***There are four major categories banned in Islamic financial transactions listed here below:***

- The first category consists of elements which are prohibited since inception; there is no debate on their legitimacy. The main practices that are considered unlawful in Islamic finance are usury (riba), ambiguity in contracts (gharar) and gambling (maysir). Riba is haram in all of its aspects. It is considered as an unjustified increment in borrowing or lending money. While gharar is banned under Islam because it is associated with uncertainty, deception and risk; maysir is forbidden on the grounds that money should be earned by way of work and effort, not involving a game of chance.

- The second category consists of elements which are prohibited if proved to be. Here remains deep skepticism over the legal interpretation of each, i.e. threat (tahdeed), mistake (ghalat), injustice (zulm), deception (khedaa), and exploitation (istighlal).
- As to the third category, it consists of a single prohibited practice in Islam because it leads to inequality, and that is monopoly or Ihtikar in Arabic. Monopoly is prevented absolutely and forbidden in Sharia.
- The last one is about fraudulent misconduct and blackmailing. Fraud literally means a deception practiced to secure an unjust gain. In accordance with the civil and criminal laws, fraud is morally wrong and is considered a crime same as theft. Blackmail is also wrong because the blackmail proposal is intimidating.

Conformity with the dictates of the revealed law is a communal obligation and prohibitions are extended to investing in alcohol, pork products and the adult-entertainment industry. Noting that the most important Islamic virtues are prescribed at both an individual and at a collective level.

Consequently, all Islamic financial transactions must be free from the above mentioned elements, otherwise transactions would be void. These salient features are fundamental of Islamic finance which distinguishes it from conventional finance.

In conclusion, although Sharia enforces certain prohibitions and imposes unique structural requirements on the types of approved investments, I believe that these features should be attractive to both the Islamic as well as any socially-responsible investor since the purpose of the above background is to emphasize that an economic and financial system driven by social-welfare and socially-responsible mandate will lead to advancing financial inclusion, and to catalyzing and promoting real economic development.

Islam assigns heavy responsibility on the human being, with just him being held accountable for any lack of development, and only him behind the reinforcement of social and economic empowerment.



# THE BIG TECH THREAT FOR FINANCIAL SERVICES FIRMS: FIVE COPING MECHANISMS

Nuxeo's David Jones discusses how Financial Services firms need to future-proof their brands against the threats from unconventional competitors like Google and Amazon

Consumer demand for personalised digital services and products is driving major changes in the financial services industry: today's consumer wants the same level of customer experience from their financial services organisations that they get from 'Big Tech' companies like Amazon and Google.

This means delivering relevant experiences to customers at every touch point possible. The products and services offered by financial services organisations are more complex than, for example, retail products, but nonetheless, consumers expect the same level of convenience and personalised omnichannel experiences they're getting elsewhere.

But that is still not the reality for the majority of customers. Most banking and financial institutions still lack the ability to deliver a truly integrated, seamless, and personalised customer experience at all touch points – whether they're visiting their bank's local branch office, standing in front of an ATM, or checking account details from their smartphone. The result is customer dissatisfaction that leaves the financial services industry wide open to disruption.

## Big Tech shaping the future of the financial services and banking industry

Disruption from Big Tech is a clear and present danger to banking and financial services organisations that stay locked into past modes of thinking when it comes to IT systems architecture, harmonising internal information systems, and the ability to rapidly build and deploy new revenue-generating solutions.

Collecting and managing the massive amount of data along all the information-rich touch points on the customer journey is a fundamental need in order for financial services firms to deliver optimal customer experiences across all channels. In other words, data-driven personalisation is the only way to deliver the level of online experience today's digital consumer has come to expect.

We recently surveyed 100 CIOs at top financial services institutions to identify the biggest challenges they face from the Big Tech threat, as well as best practices for addressing this issue. Based on this research, below are five strategies financial services firms should consider in order to compete with Big Tech competitors while enhancing and improving the experience for their customers:

### *Strategy #1: Minimise negative impacts from legacy*

Banking CIOs know that their legacy systems are impeding the flow of information within their organisations. In fact, three out of every four CIOs (75%) believe that getting access to information locked in legacy systems is vital, but most are unable to do so. Remaining tethered to antiquated legacy systems can have numerous negative consequences. Cost of ownership is only the tip of the legacy iceberg, especially when you consider the negative impacts to the customer experience. When aging and disconnected information systems serve as the foundation, credit approval processes take longer, uneven experiences across multiple channels are the norm, and dispute resolution are delayed. It's these types of less-than-optimal experiences that drive customers to take their business elsewhere.

**David Jones,**  
VP of Product Marketing,  
Nuxeo





Look for modern platforms that provide a flexible and adaptable approach for connecting to existing information systems in a manner that provides users with a single hub for storing and retrieving content and data across the enterprise. This will enable you to maximise the value of current IT investments and minimise business disruptions. Realise immediate modernisation benefits by connecting existing systems and then strategically consolidate legacy applications at your pace.

#### **Strategy #2: Greater content visibility**

Our survey of financial institutions indicates that the number one business challenge identified today is the inability to easily search for and quickly find information. Another big issue is that vital content and data resides in many disconnected systems, resulting in the proliferation of information silos.

Traditional enterprise content management (ECM) solutions have attempted to solve the information silo problem with a strategy that required all information to reside within a single central repository. However, the market has shown that the notion of 'one repository to rule them all' is not realistic, and that a more connected and intelligent platform approach where users can access information within existing legacy systems via a centralised hub. This strategy enables teams to continue to use the systems and processes that work for them, while gaining access and visibility into information systems that previously were siloed. Essentially, next-generation information management focuses on making silos transparent and accessible to everyone, rather than trying to get rid of them.

#### **Strategy #3: Link useful small systems and upgrades first**

Big Tech players like Amazon, on-demand services like Uber, and price aggregator sites like Priceline have led to new expectations for convenience, speed, and transparency that transcend industry boundaries.

For financial services organisations, part of the problem is structural: larger, older technology platforms are slow to change in response to changing market demands. One of the biggest business challenges identified by survey respondents was that it takes too long for IT to respond to requested system modifications to help optimise the business.

Becoming more agile and responsive is the only way to compete with nimble competitors who can rapidly launch new products and services and introduce improvements to the customer experience. It's a goal that can be achieved by thinking about services differently. While it may seem that the heavyweight giants such as Amazon are one large entity, they are actually made up of hundreds if not thousands of small connected pieces. Each of these pieces, or microservices in modern parlance, performs a very specific function, but most importantly connects to other, adjacent services to create an ecosystem that is much more flexible and powerful than any fixed product.

Creating an ecosystem within your own organisation may sound like a daunting task, but this concept is at the core of a modern CSP. A CSP will enable you to connect, not only microservices together but also existing, even legacy, applications that sit within your business. Connecting these silos of information together not only provides a centralised way in which to search for information, but opens up information locked in legacy systems that are traditionally difficult to use and expensive

to run. Using a core CSP to connect a range of small solutions for individual services delivers massive flexibility, corporate information agility, and the ability to leverage the existing investment in legacy systems.

#### **Strategy #4: Tame content chaos**

Financial services firms are struggling to effectively manage the massive volumes of information coming into and out of their organisations. 79% of organisations reported that they're unable to connect information from different systems. Assets exist in multiple versions in different repositories, while potentially useful data ends up in 'information graveyards', unlikely to be accessed or altered ever again. All of this only exacerbates the content chaos conundrum.

In order to tame content chaos, financial services organisations should look at modern content platforms that help break down the barriers between users and information. When structured data and unstructured content is freed from the confines of applications, platforms, and information silos, users can quickly and easily find and use the information they need to help them perform better, make more informed decisions and provide greater value to customers.

#### **Strategy #5: Prioritise scalability for future growth**

We're living in the age of the content explosion – with no end in sight.

An explosion in technologies for storing and analysing information has resulted in exponentially higher volumes of content and data being created. But no piece of information is an island – or at least it shouldn't be. The connections between different pieces of content and data are incredibly important; a customer address (data) can create a map image (content), while a license plate scan (content) can identify a vehicle owner at an accident site (data), while a customer name (data) generates a FICO score (data), or a signed contract (content) generates personalised documentation request (content).

The ability to work with a seemingly infinite number of different data types simply highlights the fact that no one knows what kind of information will become critical to a business tomorrow: will non-standard underwriting data be used to determine credit worthiness? Will social media and GPS coordinates lead to real-time claims processing? Will the expanded use of third party data dynamically change business models? Whatever the future holds, your CSP needs to be able to work with the many, many different types of information that are relevant to the business.

And whichever data type becomes critical, it's unlikely to come in small file sizes. That's why your content services platform of choice needs to scale to support ever-larger stores of content, data, and the multiple types of information created when they combine.

Modern content platforms offer financial services firms the ability to address the Big Tech threat by leveraging modern technology to work with, not against, existing information systems. By doing so, they can deliver the business efficiencies that can be achieved with traditional automated processing, but by being more flexible, agile, scalable and modern than those traditional systems they can also improve corporate agility, enhance customer engagement, and ultimately drive the revenue and profit within your organisation.

Gresham 

# THE CONTROL PLATFORM AT THE HEART OF A THRIVING DIGITAL ECONOMY

**BE DATA  
CONFIDENT**

Financial institutions with \$13Tn in AUM  
trust Gresham's Clareti platform to deliver  
absolute data integrity and control

*(that's 17% of the global market)*

[greshamtech.com](https://greshamtech.com)



**Dave Locke,**  
Chief Technology Advisor,  
World Wide Technology (WWT)





# CYBERSECURITY SHOULD BE MORE THAN A TICK BOX EXERCISE, AS REGULATIONS ARE ON THE RISE

The UK has been hit by more than 1,000 serious cyber-attacks over the past two years<sup>[1]</sup>. According to the 2018 Thales Data Threat Report, 69% of UK organisations report an overall increase in their IT security spending<sup>[2]</sup>.

Governments and regulators have updated regulations and reporting frameworks in response to the evolving threats to make sure companies can prove compliance. Regulation standards such as CBEST, MIFID2 and GDPR have increased the mandate for companies to shift from annual compliance tick box activities to delivering ongoing assurance of critical systems.

Earlier this month, as part of this strategy, the UK government identified 'operators of essential services' that will be required to comply with the security and incident reporting requirements set out in the European Security of Network and Information Systems (NIS) Directive.

The directive requires the identified businesses and service providers to ensure their technology, data and networks are secured and cyber resilient.

This however, is easier said than done. The growing sophistication of cyber-attacks requires a more robust approach to cybersecurity. It's becoming apparent that simply increasing spend on cybersecurity products is insufficient to combat the rising complexities of cyber-breaches.

With core business applications and their associated data being the biggest targets for bad actors, the first response by most companies is to segment their applications and impose layers of protection around each segment, denying free reign access to mission-critical applications across the network in case of a security breach in one part of the network. A properly implemented segmented environment can limit access by restricting lateral movement, which affords the enterprise a higher level of protection.

The underlying IT systems within these companies are highly complex, and whilst modernising them to provide vigorous cyber protection is not impossible, it is extremely difficult. These

existing legacy systems are often decades old with occasional new features added over time, forming a complex patchwork of applications. As a result, companies typically have thousands of applications that are intertwined and interdependent.

Consequently, as recent cyber incidents have shown, organisations can no longer rely on creating firewalls around super-imposed segments without understanding the specific application dependencies they are working with.

So how can this complexity be taken out of the equation? By dividing the segmentation strategy into three clear stages: an architecture plan based on risk management factors, a design with technical solutions to meet the architecture plan, and an incremental implementation process for rapid deployment.

Companies must first map out a real-time picture, or application dependency map of the entire network to understand the underlying applications and their interdependencies, the vulnerable end points within the network and create visibility across all data flows. This map can then be translated into a tailored enforcement policy for segmentation, and in turn, cyber protection. This visibility will also enable organisations to constantly monitor their network through traffic analysis and dependency monitoring and scale up or scale down the security controls as needed.

With EU-wide increases in regulatory interest around cyber defences, companies are working towards high levels of security controls and segmentation policies to protect themselves from cyber-attacks. Whilst older rules required yearly tick-box compliance exercises, new regulations necessitate continued assurance of critical applications. Insights into infrastructure can create a real-time picture of the entire network. Once this level of visibility has been achieved, organisations can confidently rationalise the way that different applications share data within the system. This means they can fit the right security policies within each segmented application, preventing unnecessary or illicit data flows that can create cyber vulnerability.

<sup>1</sup> <https://www.ncsc.gov.uk/annual-review-2018/>

<sup>2</sup> <https://www.thalesecurity.co.uk/2018/euro-data-threat-report>

# The Future Is Here



## Optimize your fraud and compliance operations with RPA from NICE Actimize!

Leveraging Robotic Process Automation results in increased productivity and investigation efficiency, while providing new insight into program effectiveness and lowering your cost and risk.

Let your team focus on the work that brings the most valuable results. NICE Actimize will show you how!



**Financial IT**  
Innovations in FinTech



**TOP 12**



**CRYPTO  
STARTUPS  
TO WATCH  
IN 2019**



# TOP 12 CRYPTO STARTUPS TO WATCH IN 2019

Looking forward from December 2018, one can see three reasons why the coming year will be a key one for crypto-currency companies.

If nothing else, the year will mark the 10th anniversary since the birth of crypto-currency, with the introduction of Bitcoin in 2009. That crypto-currencies have survived, if not necessarily thrived, suggests that they will stay around.

The second reason is that 2018 has been a brutal year for many crypto-currency traders and investors. At the time of writing, a Bitcoin can be bought for less than US\$4,000. The price has fallen to levels not seen for 14 months. Bitcoin was never a unit of account nor, really, a medium of exchange. Now it is very unclear whether it is a store of value. The coming year will likely see much greater focus on what are the quantifiable benefits from any tradable crypto-currency.

The greater focus will come from institutional investors and traders who are looking for opportunities from crypto-currencies. Significant institutional participation is the third main reason why 2019 will be an important year.

This begs the question: what are the crypto-currencies to watch, out of the hundreds that have been launched by way of initial coin offerings (ICOs) since 2016?

To select 12 crypto-currencies that, we think, will provide a clear indication of major trends in the coming year, we began with a randomly chosen group of 100 companies that are no more than two years old. We then considered:

- Market capitalization of the crypto-currency in question. All other things being equal, a high capitalization is a good thing.
- The number of coins or tokens circulating in the market. Again, the greater the value, the better.
- The governance structure of the blockchain that is being used. A decentralized structure is considered to be more reliable and secure than a centralized structure.
- Other features that really differentiate the start-up or the crypto-currency from others.

The final 12 names were those that stood out across several, or all of these criteria.

We stress that we recognize the limitations of this approach. In particular, we do not suggest that any one of the start-ups are better than any of the others, or better than any start-ups that are not included in our list.

## Sources:

<https://coinmarketcap.com/>  
<https://walleinvestor.com/forecast/0x-prediction>  
<https://investinghaven.com/crypto-blockchain/5-must-read-cryptocurrency-predictions-2019/>  
<https://www.telegraph.co.uk/technology/digital-money/top-10-popular-cryptocurrencies-2018/>  
<https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies>  
<https://cryptoslate.com/coins/eos/>  
<https://eos.io>  
<https://www.forbes.com/sites/forbesfinancecouncil/2018/08/02/how-to-start-investing-in-cryptocurrency/#6529d9d45d75>  
<https://medium.com/insightsaltperformance/in-crypto-economy-governance-is-key-8fb5430f7972>  
<https://www.cnbc.com/2018/11/23/cryptocurrencies-have-shed-almost-700-billion-since-january-peak.html>  
<https://www.cnbc.com/cryptocurrency/>  
<https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/>  
<https://www.theguardian.com/technology/2018/jan/29/cryptocurrencies-bitcoin-blockchain-what-they-really-mean-for-our-future>  
<https://www.crunchbase.com>



**Company:** EOS (EOS)  
**Crypto type:** Coin  
**Founder(s):** Brendan Blumer  
**Inception:** 2017  
**Headquarter:** South Korea  
**Team size:** 1-10  
**Blockchain governance structure:** Decentralized  
**Website:** [www.eos.io](http://www.eos.io)

EOS (EOS) is a blockchain protocol, authorized by its own cryptocurrency EOS. Founded by the creator of Steem and BitShares, the project's ICO was in June 2017. EOS is similar to a decentralized operating system, which means that developers can build applications on EOS, using its native coins. In addition, the smart contract platform claims to eliminate transaction fees and also conduct millions of transactions per second.



**Company:** Binance (BNB)  
**Crypto type:** Token  
**Founder(s):** Changpeng Zhao, Yi He  
**Inception:** 2017  
**Headquarter:** Taiwan  
**Team size:** 250-500  
**Blockchain governance structure:** Centralized  
**Website:** [www.binance.com](http://www.binance.com)

Binance (BNB) is a token, issued through the Binance exchange platform, with headquarters in Taiwan. The company has marked a steady growth since its ICO in July 2017. Binance is notable for giving its users access to a robust set of trading tools, charts and security features. Furthermore, the company is expected to enhance the operations of the Binance exchange and its ecosystem in the near future.



**Company:** Ox (ZRX)  
**Crypto type:** Token  
**Founder(s):** Amir Bandeali, Will Warren  
**Inception:** 2016  
**Headquarter:** USA  
**Team size:** 10-50  
**Blockchain governance structure:** Decentralized  
**Website:** [www.0xproject.com](http://www.0xproject.com)

Ox (ZRX) is an open and permissionless protocol that allows the ERC-20 tokens to be transacted on the Ethereum blockchain. Founded back in 2016, it enables online services to offer token trading capabilities to users without the need to hold user funds in its custody. The team behind Ox strongly believes that in the future, users will find thousands of tokens from Ethereum and that Ox can provide an efficient and trustworthy way to exchange them.



**Company:** Decred (DCR)  
**Crypto type:** Coin  
**Founder(s):** Alex Yocom-Piatt, Dave Collins, David Hill, Jake Yocom-Piatt, John Vernaleo, Josh Rickmar  
**Inception:** 2016  
**Headquarter:** USA  
**Team size:** 10-55  
**Blockchain governance structure:** Decentralized  
**Website:** [www.decred.org](http://www.decred.org)

Decred (DCR) is a crypto-currency that focuses on community input, open governance, sustainable funding, and development. It uses a hybrid "proof-of-work" and "proof-of-stake" mining system to ensure that a small group cannot dominate the flow of transactions or make changes to Decred without the input of the community. It claims that the integrity of the currency prevents people from making fraudulent transactions.

5



**Company:** TrueUSD (TUSD)  
**Crypto type:** Token  
**Founder(s):** Rafael Cosman, Stephen Kade, Danny An  
**Inception:** 2017  
**Headquarter:** USA  
**Team size:** 10-50  
**Blockchain governance structure:** Decentralized  
**Website:** [www.trusttoken.com](http://www.trusttoken.com)

The flagship token of the TrustToken platform is named TrueUSD, and it claims to be a one-to-one exchange for U.S. dollars. TrueUSD is the first of what the team hopes will be many asset-based tokens on the TrustToken platform. It is a USD-backed ERC20 stable coin that is fully collateralized, legally protected, and transparently verified by third party attestations. It uses multiple escrow accounts to reduce counterparty risk and to provide token-holders with legal protections against misappropriation.

6



**Company:** Steem (STEEM) 41  
**Crypto type:** Coin  
**Founder(s):** Ned Scott  
**Inception:** 2016  
**Headquarter:** USA  
**Team size:** 1-10  
**Blockchain governance structure:** Centralized  
**Website:** [www.steem.io](http://www.steem.io)

Steem (SMT) is a cryptocurrency, used to power Steemit, an incentivized blockchain social media community. It is a digital asset, developed on the Steem blockchain platform, which can be launched by anyone to monetize online content. It is similar to Ethereum's ERC Tokens, but with certain built-in "proof-of-brain" properties and a token distribution reward system that is specifically designed for the given area.

7



**Company:** Dentacoin (DCN)  
**Crypto type:** Token  
**Founder(s):** Dimitar Dimitrakiev  
**Inception:** 2017  
**Headquarter:** Netherlands  
**Team size:** 10-50  
**Blockchain governance structure:** Decentralized  
**Website:** [www.dentacoin.com](http://www.dentacoin.com)

Dentacoin (DCN) is an Ethereum-based utility token, which can be easily exchanged with other crypto. It is the first blockchain concept, designed for the Global Dental Industry. Dentacoin develops market intelligence through a cryptocurrency reward system that inspires participation throughout the community. Also, it is the first crypto-currency that deploys a decentralized review platform and transparently rewards patients and dentists, who make contributions that benefit the community.

8



**Company:** Nebulas (NAS)  
**Crypto type:** Token  
**Founder(s):** Hitters Xu, Aero Wang  
**Inception:** 2017  
**Headquarter:** USA  
**Team size:** 10-50  
**Blockchain governance structure:** Decentralized  
**Website:** [www.nebulas.io](http://www.nebulas.io)

Nebulas (NAS) is a search framework for finding information on decentralized blockchains and smart contracts among the vast cryptocurrency market. The project highlights its self-evolving and upgradable smart contract capabilities. Nebulas contributes to solving challenges of interoperability, improving DApp quality and prevention of 'hard fork or soft fork'. The Nebulas team is proud of good standing, tech advancements, and collaborative spirit that help to strive forward.





**Company:** Red Pulse (RPX)  
**Crypto type:** Token  
**Founder(s):** Jonathan Ha  
**Inception:** 2015  
**Headquarter:** Hong-Kong  
**Team size:** 10-50  
**Blockchain governance structure:** Centralized  
**Website:** [www.red-pulse.com](http://www.red-pulse.com)

Red Pulse (RPX) is a tokenized research ecosystem that uses its own crypto-currency. It is an event-driven research startup that delivers its services in real-time via web portal [red-pulse.com](http://red-pulse.com), iOS app, email and partner distribution platforms. This way Red Pulse provides analysts, investors, traders, and advisers with the edge, they need to make better-informed decisions, and its own cryptocurrency is there to enhance the process.



**Company:** QLC Chain (QLC)  
**Crypto type:** Token  
**Founder(s):** Susan Zhou  
**Inception:** 2017  
**Headquarter:** Singapore  
**Team size:** 1-10  
**Blockchain governance structure:** Decentralized  
**Website:** [www.qlc-chain.com](http://www.qlc-chain.com)

QLC Chain (QLC) is a crypto-currency, designed to facilitate the peer-to-peer transactions of telecom services on the platform. Users need to pay QLC tokens to use services, provided within the QLC ecosystem. It is the next generation public blockchain for decentralized Network-as-a-Service providers. The QLC Chain and supporting ecosystem enable any individual, business, or organization to leverage infrastructure and mobile network resources to instantly become a service provider or network operator.



**Company:** Dropil (DROP)  
**Crypto type:** Token  
**Founder(s):** Zachary Matar, Jeremy McAlpine  
**Inception:** 2018  
**Headquarter:** USA  
**Team size:** 1-10  
**Website:** [www.dropil.com](http://www.dropil.com)

Dropil (DROP) is an autonomous trading investment platform that brings autonomous financial planning and investing to the cryptocurrency world by offering long-term investments, short-term investments, and retirement plans, claiming that they are better than any investment opportunity in the world. The team strongly believes that the best work comes from the heart without decisions being diluted by boards of directors. This allows staying focused on the goals and delivering the best value.

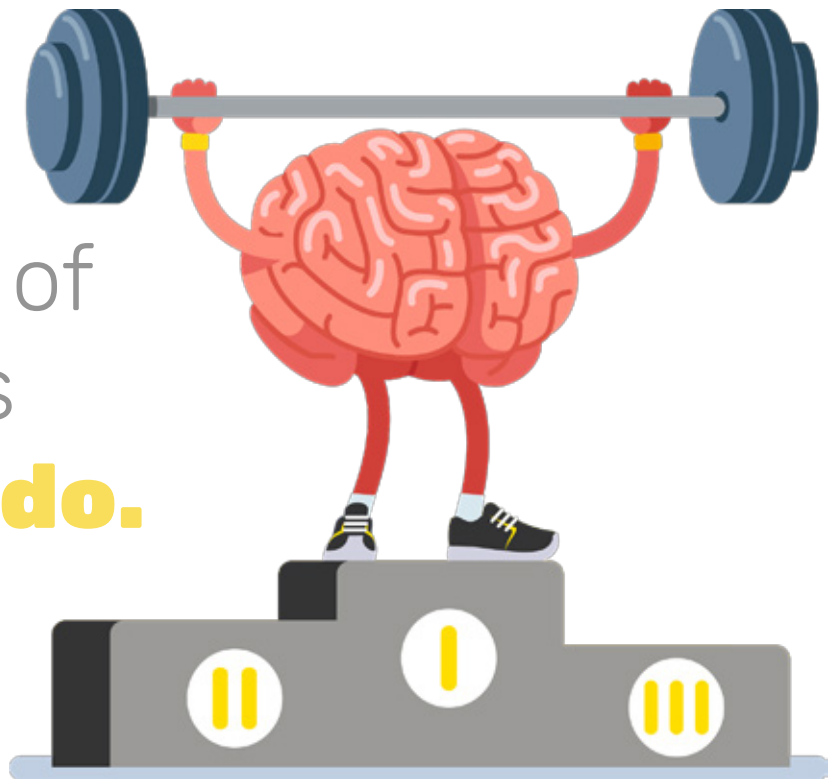


**Company:** Tokenomy  
**Crypto type:** Token  
**Founder(s):** Oscar Darmawan  
**Inception:** 2018  
**Headquarter:** Singapore  
**Team size:** 10-50  
**Blockchain governance structure:** Decentralized  
**Website:** [www.tokenomy.com](http://www.tokenomy.com)

Tokenomy (TEN) is a worldwide token platform for crowdfunding, loyalty points, and reward programs. Its goal is to create financial inclusion and provide access to anyone, who wants to be connected with alternative funding and global innovation. In addition, it is a one-stop tokenization platform that allows individuals or corporations to generate, distribute, and exchange their tokens. Tokenomy also provides a marketplace for other valuable tokens to be listed and traded on the crypto-only exchange.

# PAYBASE\_®

Raising the bar of  
what payments  
**can & should do.**



**[ Don't take payments. Own payments. ]**

Paybase provides an end-to-end platform that covers payments, compliance and risk management. Specialising in payments between multiple parties, Paybase is perfect for online marketplaces, gig/sharing economy platforms and products with sophisticated payments requirements.

By offering the most flexible solution on the market, we allow businesses to build the platform they really want, removing payments as a barrier to innovation.

Learn more at [paybase.io](https://paybase.io)