MONEY 20/20

EUROPE
21-23 SEPTEMBER
AMSTERDAM

Think Tank Reports 2021

Table of Contents

Fintech's biggest challenges will not be solved by a single person or company. It takes a community. And that's where Money20/20 Europe comes in. Our Think Tank programme created an immersive agenda feature bringing together six groups of up to 15 selected industry players to ideate and co-create a solution for the most complicated problems we face together.

While the think tanks themselves are epic, the process was beautifully simple. Each of the 6 think tanks operated under Chatham House rules, so participants could feel free to say what was necessary. At the same time, detailed notes were taken so we could deliver recommendations from the discussion to be shared with the industry here.

For many of our questions, the discussions and recommendations included in these reports are merely beginnings. The conversations will continue online, at other events, hopefully face to face, and eventually, back at Money20/20 Europe in 2022.

How would we interact with money if banks didn't exist?

If we were to design the world of finance from scratch, how would we go about it? Without assuming the necessity for the existing structure of the industry and current forms in which we access, transact, and manage our financial assets, how would we design the way we interact with money? How do we do it in a way that is conducive to fast, safe, and sustainable progress in the financial services industry and beyond it?

PARTICIPANTS:

Leader: Matthew Locsin
Group Vice President,
Global Head of Innovation,
Publicis Sapient

Roland Folz
CEO,
Solarisbank AG

Yorick Naeff
CEO & Co-Founder,
BUX

Ahmed F. Karsli
CEO,
Papara

Hristian Nedyalkov
Co-Founder & CEO,
Novus

WHY HAVE THIS DISCUSSION NOW?

The need for banks as the primary financial intermediary has passed as embedded finance and increased technological efficiency have changed the economics. Lower barriers to entry in banking foster competition, which strengthens the market. Banks are still trusted, owing to government deposit insurance, yet safeguarding money is still possible without government involvement.

WHAT WORKS AND WHAT SHOULD WE FIX OR BUILD?

Banks have historically differentiated themselves on products, but customers think in terms of ecosystems, where they can get added value. They arrive at a transaction, but only at the end of that journey through an ecosystem.

The manufacturing mindset is endemic and to combat that banks must forget the product and focus on optionality. People want personalized experiences and value alignment from their service providers, especially in the medium term.

> Banks should be allowed to charge where there is added value and even then, according to how that value is perceived.

Originally a store of value, money's role in society is as a transactional means to an end. How then can we ensure customers can do what they want in an ecosystem? Banks be reduced to managing money and flows, but that is the root of the product mindset. In traditional banking's defense, this is an inherent conflict because such an ecosystem approach provides a means for customers to consume rather than fostering a business model.

IDENTIFIED NEEDS

Current levels of transparency are passable, but the pandemic has changed expectations. This generation has more options and better access to data, which means banks cannot afford to be less transparent. Today, customers would simply delete an app and download another.

A degree of rules and regulation is required to support transparency and accountability. However, banks have been reluctant to support those needs. Changes are already possible in terms of faster account opening, not processing payments in batches, and improving nationally fragmented consumer credit laws. Banks do not change these processes because it is not in their interest to do so.

Banks can operate for a societal purpose, however, they have been operating in preference for their shareholders' returns. If banks, or their future inheritors, foster a feeling of being part of a community, it could be powerful. Alternately, we can reposition banking as a different type of player: for example, a government institution with a social remit.

TECHNOLOGY

The clearest change to financial technology is decentralized finance, or defi, but there are other ways to solve the transactional side of money. Centralized infrastructure enables a few banks to dictate terms, but defi architecture would allow us to iterate faster and better. Scaling defi solutions will take much more time, with embedded finance likely paving the way for defi. Defi also holds the promise of potentially removing the risk of institutions that are too big to fail.

New technologies enable banking at a better cost base, however, ecosystems will integrate financial services in their offering. Below that is a level where someone will provide a universal regulatory and technology layer. Regulators have scrambled to create policies to address what new technology enables, and some policies have missed the mark.

SOCIETY

Banks should be invisible service providers where decentralized or fintech players have the relationship with the customer. The purpose of collecting and lending money is still valid and should still be regulated. What we need to change are the transaction costs. Banks should be allowed to charge where there is added value and even then, according to how that value is perceived. More sophisticated pricing models are required to achieve this, as individual consumers need and value different things.

Banks have a role to play in how money is thought of and utilized, and it should hopefully be an educational role. Customers should know what their deposits are used for and whether that lending has enabled people to do activities that match your values. Banks should aim to improve equality of access to financial services. Customers with high balances can access many services for free, but a customer with low balances has to pay for everything.

The future is trustless. What do we need instead?

Trust is an outdated concept. We should not need trust to be able to do trade and share. Trust should be an implicit hallmark, not an explicit task. What do we need to develop to remove the need to achieve it? And what do we need instead? We need to build an environment that is safe by default. We need to shift from transactions based on the identification of the counterparties to transactions based on the strongly authenticated credentials of the counterparties. How do we get there?

PARTICIPANTS:

Leader: Dave Birch
Global Ambassador,
Consult Hyperion

Felix Gerlach
CPO & Co-Founder,
Passbase

Greg Storm
Co-founder & COO,
TripleBlind

Katryna Dow
CEO & Founder,
Meeco

Louise Maynard Atem
Research Lead,
Women in Identity

DON'T TRUST, VERIFY

A few foundational truths inform our discussion. First, verification tells you nothing about the type of transaction you're trying to execute. Second, knowing your identity doesn't help a counterparty know what you are. Finally, identity fraud is rampant and has only been accelerated by the pandemic.

IF I'M DRIVING THE CAR, I STEER. IF I'M BEING DRIVEN, WHO STEERS?

One of the key aspects we have to change is identity. Identity has historically been handed out by governments, but more identity assets are needed to prove your identity and demonstrate an identity history.

If we move to the world of Verifiable Credentials, then we don't have to lecture people about changing their passwords and we can help protect them. These credentials, however, have to be consistently weighted so we know how to value them when we aren't familiar with them.

The value of verifiable credentials is about consistency over time. Habit and reputation increase the value of a credential over time. For example, if my AirBnB or Uber rating is un-gameable and is cryptographically protected, why can't my bank access that?

Many of us are far too irresponsible to be given control of important things, such as our identity or verifiable credentials. For the vast majority of people, an infrastructure must be created to control and protect them.

WHY CAN'T BANKS MANAGE MY DATA THE SAME WAY THEY MANAGE MY MONEY?

Which is worse, to lose my money or lose my identity? Probably, identity. Banks should be putting more effort into protecting my identity rather than my money. Banks can already provide a tokenized handshake for data exchange with third parties. But in what scenarios should the data be shared between the multiple parties that together generate transactional data along with the platforms that underpin those transactions? Would you pay the bank to provide you with a tokenized account of all of your transactions?

As soon as other entities trust a system, it can work. In the crypto world, for example, people trust the cryptography. We should build a system that is open and tested, where one set of tokens can be interchanged with another system's tokens.

Finally, how many trusted networks do I need? Passports used to be a universal piece of information for all I needed to do. However, multiple networks may give us more resilience.

WHERE WILL THE BREAKTHROUGH COME FROM IF NOT FROM THE BANKS?

Hopefully, we will see a privacy switch, similar to the Negroponte switch, where we reallocated TV connectivity to wires and phone connectivity to the air. Privacy technology needs to be more useable and proveable.

An interoperability framework is necessary to make sure we can incorporate all players into a framework that enables new players to build value on top. Trust anchors, such as banks, will need to lead this process because they have governance, boards, regulation, etc. The reason for working with banks is that the alternative is technology companies that have no accountability or regulatory oversight.

> The reason for working with banks is that the alternative is technology companies that have no accountability or regulatory oversight.

Should banks be the party to provide the infrastructure for all of this? There has been a shift in who we trust. After 2008, many don't trust big financial entities. Looking forward, decentralized finance, or defi, gives us an alternative to centralized trusted actors, which should also work for a trusted identity layer.

WHAT'S THE PATHWAY INTO THE MARKET FOR CREDENTIALS?

Contrary to what some may think, individuals and businesses actually do trust banks because they still use them. Therefore, banks could act like the NHS in the same way we trust health/vaccination credentials. Some institutions may be trust anchors, which operates differently from cryptographic trust.

Alternately, trust in this world is linked to customer sovereignty, so why not an individual instead of a bank? There is an evolution toward a custodial service from banks, including toward data and identity. Even sovereign identity documents need to be linked with external actors who can add value to my sovereign identity. If there was an API of me, my digital twin, then I can delegate others to act on my behalf.

We should seek to strengthen this network of networks, building a fully transparent and open-source system where people understand how we compute trust. Transactions are three things: counterpart, mechanism, and intermediary. As soon as we solve a portable KYC check, we can move into a trustless response.

In a world where cards don't exist, what should a payment solution look like?

If we stopped iterating existing payments solutions but designed them from the ground up to address the needs of customers across a variety of contexts they transact in, what would modern payments solutions look like?

PARTICIPANTS:

Leader: Pablo Tramazaygues
Partner, Financial Services EMEA,
Retail Business Banking,
Oliver Wyman

Evgenia Loginova
Founder & CEO,
Radar Payments by BPC

Oded Zehavi
CEO & Co-Founder,
Mesh Payments

Gian Battista Baa'
Head of Digital Payments
& Services,
Intesa Sanpaolo

Henry George
CTO,
Trilo

Andrew Takyi-Appiah
Managing Director,
Zeepay

Tatiana Rozoum
Co-founder,
Fintecture

Andy Wiggan
VP Product Management,
GoCardless

Francesco Simoneschi
CEO,
TrueLayer

WHO IS IT FOR? WHAT DOES IT NEED TO DO?

The future of payments will be seamless and frictionless. Wallets are still underpinned by cards; but outside of cards, account to account, instant payments running on QR codes are replacing this, especially in geographies where cards are less prevalent. As well, blockchain and crypto-secured payments systems are proliferating.

Historically, cash was the transfer of value for consumers. Over the last 70 years, complexity was added to the simplicity of cash's value transfer. We have the chance to design a simple system without all of today's caveats and instant payments are the way to do that. Corporates, on the other hand, hate the form factor of cards, but even when actual cards aren't used as a token, it still relies on the card rails.

It's difficult to replace the ubiquity of the card rails. Apple had the last great chance to create an alternative to the card rails. Innovation and niche solutions on the existing rails will come, but it will be difficult to disenfranchise Visa and Mastercard. In an open banking world, competition increases, and therefore, the speed of innovation should improve.

Looking at the retail experience, the expectation used to be that commerce would happen in person, via bank accounts, and physical wallets, but now, phones are the starting point. APIs are now fungible and security design is ready for peer-to-peer trust instead of relying on a centralized entity.

There will be a natural evolution of cards into wallets. in terms of the payments infrastructure, we will move to electronic funds transfer, which has evolved differently in different geographies. However, the infrastructure is still catching up and the question becomes which geography will move forward faster? In the European Union, innovators are leveraging the card rails, but the wallet rails offer far more possibilities. EMI is essentially a wallet with rules set by the regulator rather than by an operator, which increases the degree of consumer acceptance and trust.

WHAT WILL BE THE MAINSTREAM AND HOW LONG WILL ADOPTION TAKE?

We have to develop solutions to follow customers. The existing card infrastructure enables an ecosystem that allows customers to do what they want wherever they want, with whoever they want.

The critical innovation, however, should not be about the device or vehicle, but about the foundation for building multiple payment solutions that address different needs. The foundation must allow diverse participants to reconcile in-store and online and be cross-border, so standardization is important.

We also need to anticipate the behavioral change that will happen and build for what we anticipate. Once we work for the behavioral change, we have to build value on that changing behavior.

Questions remain about who pays for the infrastructure that supports open banking because we will still need infrastructure and rules.

HOW LONG WILL IT TAKE TO CONVERT THOUSANDS OF BANKS AND REGULATORS IN EUROPE?

Technology is the least of the problems to solve for payments innovation. Innovation likely has to come from big players or governments. We let governments provide us with utilities, so why not a payment infrastructure as a utility? Otherwise, it will evolve on its own as soon as there is a strong enough market player.

Aside from the policy aspect, any discussion around infrastructure should not be about technology, but the consumer behavior and then the mechanisms that enable it. Consumers have already made a choice to use wallets and super apps. The next generation will likely consider those as their native payments platform.

Convergence of wallets and card rails will happen through government legislation but even more so through the businesses that combine payments through open API ecosystems. Consider what would happen if Apple bought iZettle and owned the merchant and the consumer accounts. This shift will likely only happen because of some large brute force, like a FANG stepping in and pushing it forward with the massive amount of relationships and data they already have.

With open banking, we will have common rules and acceptance of new services for new customer solutions. In the future, there will be a few payment methods and ecosystems, rather than a single, global point of convergence. At the same time, consumers do not want complexity; they have a limit to how many apps they will use.

Consumers will ultimately decide which platforms or services to use based on environmental factors and frankly, what's cool or attractive. The average user doesn't care about payments: they just want value. Consumers are not loyal to anything that doesn't solve a problem, which is a fundamental stimulus for anything that delivers improved outcomes. This disloyalty may be one of the few things strong enough to overcome the card rails' network effects.

Merchants have a higher network lock-in factor, which is why they pay the bill for many innovative consumer experiences. That's why the business model has to change and competition has to be increased.

Even if we start with consumers, once we move to cross-border we must consider the opinions of governments and regulators. Cross-border e-commerce and travel will only emphasize the role of governments. Some global powers with their own agendas might be able to accomplish this transition in collaboration with a few others.

Single rails will have to adopt multiple payment instruments. Adoption will likely be led by mobile wallets as we use our phones for transactions rather than entering an app that requires a source of payments. One app will enable a payment that starts on one rail and ends on another. Linking ecosystems will allow us to include more people in payments.

What should an open data economy look like?

With the inevitable progression from open banking to an open data economy, the financial services industry can play an important role in becoming the trusted core for the orchestration of data and payment flows between industry players. Let's move beyond open banking and map out what the industry would look like if we were building an open data economy. How will the competitive structure change? What will be the role of financial organizations? How will it change the technological fabric on which the financial services are built and delivered?

PARTICIPANTS:

Leader: Louise Beaumont
Chair, Advisor, Speaker

Elise Johnsen Kirkhus
COO,
Neonomics

Jack Wilson
Head of Policy,
TrueLayer

Yasamin Karimi
Head of Product,
Codat

Ron Carey
Head of Product,
Yapily

Anil Hansjee
General Partner,
Fabric

Rune Mai
CEO,
Aiia

Katja Hunstock
CPO,
finleap connect

Sam Seaton
CEO,
Moneyhub

Marijke Koninckx
Chief Product Officer,
BankiFi

Denise Johansson
Co-Founder, CCO & Deputy CEO,
Enfuce Financial Services

The first step is to define the supply and demand side between data creators, holders, and users, which raises the issue of sequencing and what to build first: networks or funding?

CONSTITUTION

We must decide whether rules for the data creator, holder, accessor, and user should be voluntary or mandatory. We must determine if the open data economy concerns originating data or metadata and whether data originators can remove metadata.

As it is, consumers generate data but it gets locked up with a provider. Customer data needs to be used to empower the consumer and not be hoarded. However, an investment firm, for example, will be reluctant to give access to data around customer investment choices.

Under the open banking regime, the value was transferred away from incumbents, which led to friction in adoption and experiences. In transport or content or journalism, open data has worked because there was a natural understanding of the win-win scenario. Open banking rules are meant to increase competition, and the ecosystem is already developing, but it's not regulated. In financial services, most incumbents are scared of losing what they have rather than thinking about what they could do.

> The commercial value of open data is massive, but market forces working at their own pace will mean it doesn't come soon enough.

It took regulators forcing the hand of banks toward open banking. Even with the regulations, it hasn't done enough because there are excuses in how those regulations can be interpreted. It will eventually take market forces to create a business model with virtuous cycles in supply and demand to achieve long-term success.

Has the regulation gone far enough to allow the market forces to take over? There is a carrot and a stick dimension to creating new experiences, but there is an increasing awareness that the data should be the consumer's and that they should have oversight into how that data is monetized. Value creation will lead to funding.

If we didn't have regulation, there wouldn't be trust for everyone to participate in open data ecosystems. Therefore, regulators play a foundational role but don't offer enrichment. New fintechs that openly share data and are transparent about the purposes of that sharing will win. In the end, the consumers will pay for it.

Looking at the business model, there is a disconnect between people who create data and the value creators, but we can't create an open data economy without controllers and access providers. For those that provide access, it's an easy business model. For data holders, however, there is no financial incentive, especially under open banking.

With financial data, the data controllers are more sensitive owing to financial regulation. And it's not just hesitation from data controllers. The Dutch government commissioned a survey that found hesitance from consumers around sharing their financial data. We need to ensure we can better the lives of Europeans with better data sharing, which PSD2 did not achieve.

How then do we incentivize participants and break down the risk of my data being corrupted? Regulation can make consumers more likely to trust new solutions, but how do we incentivize the providers?

This can be market-led. Consider, there were monetized API economies before PSD2; for example, using Google maps data. Although banks have been disintermediated from some transactions, open data can allow them to gain more details about their customers.

Most banks won't be able to deliver on this vision of an open data economy because they are not aware of what data they have. Banks' strategic decision-making is also not focused on this, as they react to perceived present competition. Banking oligopolies need to be broken down and the fountain of data held between them unlocked.

The best regulation that could happen would be to decimate banks and split them into component pieces. Regulators could move this forward faster, but more often than not, they respond retroactively to issues in the market.

So what are the alternatives? Defi offers a new set of mechanisms to monitor transactions and movement of data, but that is 10+ years from realization. Meanwhile, tech companies are unlikely to create a genuinely open data economy, as evidenced by the fact that Google doesn't allow consumers to access their data. Technology firms abide by the regulation but not it in a way that empowers consumers.

The commercial value of open data is massive, but market forces working at their own pace will mean it doesn't come soon enough. Having considered the options, we still need a kick in the butt from the regulators.

A SUCCESSFUL OPEN DATA ECONOMY

We should aim for a hyper-personalized, predictive, and preemptive service. It should be pleasurable and not biased in any way. The goal should be that the end-user sharing their data that has a safe enough environment to share it. Customers should also be allowed to revoke access to their data.

> We need either regulated information warehouses, like in the derivatives markets, or synthetic data that others can use.

The business model becomes clearer as transparency drives customer choice. Most customers don't understand the financial value chain and the margin extracted by payments banks, for example. Price is an ultimate measure of success, and if it leads to price improvement for consumers, we know it has worked.

An open data economy would be highly attractive to innovative investment in light of the potential for better business models. Established organizations would want to base themselves in open data economies because they see the value. Individual consumers benefit from better services and products. At the same time, bad actors lose out because it's harder to do wrong.

An example of the value for consumers and institutions is in fraud and crime prevention. Improved data sharing would enable banks to reduce their risk and thereby theoretically decrease costs passed on to consumers.

The heart of value creation in an open data economy is the power of personalization. The value exchange comes from making products relevant to consumers exactly when they need them.

NEXT STEPS

We need a GDPR 2.0, where we can be more open with data usage for legitimate purposes. We need either regulated information warehouses, like in the derivatives markets, or synthetic data that others can use. A GDPR 2.0 would need to make data portable, instant and transparent.

More joint work should be done to educate consumers and celebrate the improvements in specific use cases for them. The UK's Competition and Markets Authority has been advertising these wins in the UK. Transparency will be a big driver of consumer adoption.

Regulators will benefit from further education and advice as well. Often they are unclear what the impact of their regulations may be. Regulators seem unclear, for example, about the line between convenience and advice, such that financial firms are worried about making recommendations if they will not match suitability rules.

On the business side, we need to create a smart data right and regulate what access to that looks like. The ecosystem for business data is more complex, especially if you include the world of accounting.

The development of the open data economy will be more evolutionary as great experiences are developed. The industry must continue to innovate to create new user demand and continue to put pressure on data holders. Ultimately, we need to strive for societal benefits and a system that's fit for purpose.

What infrastructure do we need to build to enable individuals to control their data and assets in all of their variety?

As an industry, we know how to manage a very limited range of assets, but it will change fast. Personal behavioral data, health data, programmable money, identity, etc. - are all assets we should have control over. Everything we can exchange and generate when interacting with platforms is an asset. What technology and infrastructure do we need to develop to enable that control?

PARTICIPANTS:

Leader: Alexander Koppel
CEO,
RIDDLE&CODE

Thomas Otendal
Head of Group Treasury,
Saxo Bank

Lior Lamesh
CEO & Co-Founder,
GK8

Max Boonen
Founder,
B2C2

Michael Shaulov
CEO & Co-Founder,
Fireblocks

Jean-Marc Stenger
CEO,
Societe Generale - FORGE

Graham Rodford
CEO,
Archax

Jan Brzezek
Founder & CEO,
Crypto Finance Group

Adrien Treccani
CEO & Founder,
METACO

Oleg Kurchenko
Founder & CEO,
Binaryx

Petr Kozyakov
Co-Founder & CEO,
Mercuryo

Dolf Diederichsen
Co-Founder & CEO,
Hyphe

HOW DOES REGULATION INFLUENCE STRUCTURE INVESTMENT?

Infrastructure investments are heavily biased by the expected regulatory environment, which is why we need to explain to regulators about self-custody or direct custody. That said, the regulatory environment has progressed a lot even since 2018. US regulators are competing with each other making it hard for crypto companies to enter the market. The US is a mess right now, but the Biden administration is much more engaging.

In terms of funding new infrastructure, venture capital firms are not bothered by regulatory uncertainty - it's just a bump on their time horizon. Working with tier 1 banks is beneficial because they already actively work

with regulators and have better discussions with them. Apparently, regulators in the US prefer incumbents over firms like Uniswap because they think they can control incumbents better. Working closely with banks, joining them in conversations with regulators and making adaptations in the technology layer will foster regulatory confidence in the crypto industry.

Compared to the regulatory competition in the US, in Switzerland, one regulator got in early and built up expertise, which means they approve licenses much faster. Germany, on the other hand, is not advancing. Meanwhile, Switzerland's FINMA is cautious, meaning we can't deploy new features as soon as they're ready. The entire infrastructure discussion is predicated on the speed of regulator, rather than technological development.

Thus far, the crypto industry has failed at cultivating beneficial regulations. Going forward, the right approach should be finding common ground as we're missing a common language and the clarity and transparency that come from that.

Consider how hard it is to get a bank account as a crypto company. It may create a business moat for some, but has hindered broader development of the industry. Localized registrations across Europe have made it extremely onerous to expand, such that it's hard to sell this to banks and institutions. The industry needed to communicate better and proactively shape regulation.

Before five years ago, a crypto firm could work from one license around the world, but now you need a license in every country where such licenses appear. In five years, the whole market will be covered by licenses creating a market for providers to enable efficient access.

Crypto asset permissions cannot be passported which shows a lack of maturity from the regulators. We want to be cross-border but we have to apply for a new license in every jurisdiction. Meanwhile, Binance can innovate and pay tax offshore. Rather than resist this disruption, regulators need to get ahead of this and cooperate to remove the incentive to operate in the grey area like Binance.

Identity and KYC is a priority issue to address and find clarity with regulators. The problem of payments is also the problem of identity. It's unlikely consumers will trust the governments to take these details back, but what about banks? Why would people trust banks to do something that isn't in the banks' self-interest? The solution might be a consortium of banks providing an identity and KYC solution.

Open banking will eventually expand into ID sharing, but if we pursue a European blockchain for identity data, it would likely take 5-10 years to realize. KYC verification is the first problem for crypto companies to solve, as it will allow regulators to directly connect to the database and automatically pull the information they need.

We need to understand the commonalities of individual regulators because they are speaking with each other, coordinating and adapting frameworks from each other. The result is that when a firm gets a license under principles-based regulation, they then implement it globally because they only want one system. The problem is when there are contradictory regimes. There is a lack of standards even inside Europe.

Another issue is that regulators expect crypto firms to follow the same rules as traditional asset classes. Working closely with banks, joining them in conversations with regulators and making adaptations in the technology layer will foster regulatory confidence in the crypto industry.

WHAT INFRASTRUCTURE NEEDS TO BE BUILT?

The Swiss market is already quite fragmented in that there are many different needs. The main thing we see is the need for modularity by jurisdictions and processes. The best approach would be to create foundational layers we know are common as well as best practices around key management and storage to align requirements across jurisdictions.

Regulators are completely fine with digital bonds, if not crypto. Tokenized traditional assets will be accepted faster than other digital assets, which is why tokenized assets should run simultaneously with crypto assets as new asset class. Societe Generale has placed a tokenized bond via the public Ethereum network, which the regulators feel more comfortable because it resembles familiar securities.

In Europe, things are moving in the right direction: e.g. the pilot regime for security tokens. What is missing is a common language and clarity among participants to begin building common services that can talk to each other along the value chain. Infrastructure must be able to adjust to all circumstances as the challenges are similar in every country, but the execution is different.

For banks, asset and settlement are different in the digital asset world. Traditional banks will be truly disrupted and we may see a Kodak effect for some incumbents. That said, there is a strong convergence between native crypto players adding traditional financial capabilities and some traditional banks incorporating crypto expertise.

Holding crypto assets is a 100% risk weight in the view of many banks, so having tokenized bonds instead of traditional bonds has a positive effect on risk management. Also, there is no spread to be earned, so everything sits in the post-trade cost structure of the business. We need the infrastructure, but we also need a business model to support the risk weighting.

Client demand for crypto is there, as is the demand for tokenized assets from banks. When you talk to a

bank about crypto trading, it's a revenue source. When you talk to them about digital assets, it sits with the innovation lab, so it's harder to get those services and products into production.

We talk about how we need to improve bank settlement, but we need to create an infrastructure for tokenized assets and then the rights of non-digital assets can be tokenized, which ensures the settlement of those rights is done correctly.

If you talk about the future, it's clear that defi projects are the most exciting and directionally correct infrastructure. The biggest issue is there is one world of crypto and another of tokenized securities. If your firm touch securities, you have to be regulated and become a broker-dealer, which limits the innovation in that space. Consider the opposite case to make this clearer. If tomorrow, Binance issued a tokenized bond, it would be 10x oversubscribed. There is so much money behind Tether because crypto market participants have no trust in banks.

In the end, we're building two parallel infrastructures: the neobanking infrastructure and the regulated world. Banks are all curious about blockchain, but the ones that moved forward were the ones interested in crypto as that is the only revenue source. For tokenization, there is no reasonable business case for tokenization on the blockchain because they just do so on private blockchains citing information security. Banks should stick with cryptocurrencies.

We shouldn't underestimate the infrastructure we're building. The pipes can support any token or asset, but they aren't fully utilized. In terms of tokenization, we see massive value creation for clients as a way to create a global marketplace that enhances the financing opportunities for companies seeking finance; for example, investment managers accessing fractional assets they can't access now. We see value in 24/7 market access as defi protocols smooth operations and enable greater efficiency and profitability.

True blockchain technology can only come with a public blockchain, born in the world of open-source. Common standards and interoperability will be essential, but the first step is to reengage to create a common language to allow clients to move between providers to grow the industry first. Only then should we build competition.

The industry should set standards around who should store private data and create a data exchange and then take them to the regulators.

IN THREE YEARS' TIME...

Banks started as vaults in a village and then added layers of complexities and services. The layers then became the source of revenue instead of the vault. Banks may see a parabola and return to money from storage because they can't afford to miss the opportunity and only become a digital vault. Anecdotally, we're already seeing heads of crypto at banks applying for roles at crypto firms. Hopefully, banks will build and address the fragmentation in the crypto market.

If banks will not engage, they will miss out on an entire economic generation. On the other hand, if they start with custody, they can build staking, defi and NFTs on top of that. Otherwise, banks will be limited to trading crypto, but only as minor players.

Non-financial companies are already trying to transform their assets into digital assets, but many won't finish the migration until regulatory standards become more clear.

We're seeing the convergence of crypto with traditional financial services with the result that some assets will be categorized and regulated. Despite that, half of banks still may not offer accounts to crypto firms.

CBDCs and digital wallets will provide the financial infrastructure we can operate on. With a digital wallet that includes every asset and personal control of those assets, Coinbase and the like will be ready plug in their APIs. We must build a digital infrastructure where consumers buy crypto at any broker, which will then enable the provision of access to investment classes many consumers do not currently have access to.

In the future, we'll just talk about assets on the blockchain and all the non-bankable assets we have on the blockchain, both as a person and a corporation. Assets and personal data will be given value and others will be allowed to extract value from it.

The value in crypto will not be in coins, but in cross-border payments and CBDCs where digital assets are the rails for processing payments. Crypto trading margins will reduce significantly, so payments will be key to the business model. The appetite of banks to go into that space will be determined by where central banks are on their journey toward digital assets. If cash can flow into the digital space it will change the whole picture.

Building the bridges in the financial ecosystem will, in turn, build bridges to energy, mobility, and other data products including the machine economy. NFTs or incentivized models will encourage the technology firms to move into new digital products. Imagine if tomorrow Facebook announced that attention can be used to mine Diem coins.

We're entering a new era of transforming physical objects into digital copies, tokenizing any kind of machines.

What's the least number of times you can have a customer prove their identity?

The industry standard is the assumption that the burden of proving one's identity is on the customer. And all of our interactions and experiences are built to start the relationship with the request to prove one's identity and eligibility. How would the products and our interactions with them change if we started from the assumption that the burden of proof lies with the company and the product instead of the end user? What technologies, flows, and partnerships do we need to build and use to allow customers to never have to prove who they are?

PARTICIPANTS:

Leader: Andrew Bud
Founder & CEO,
iProov

Krik Gunning
Co-Founder & CEO,
Fourthline

Fabian Eberle
Co-Founder & CEO,
Keyless

Kaarel Kotkas
Founder & CEO,
Veriff

Eduardo Azanza
Co-Founder & CEO,
Veridas

Liudas Kanapienis
CEO & Co-Founder,
Ondato

DO WE ACTUALLY THINK IT'S A GOOD THING TO VERIFY ONCE?

Initial Identification is already done well, but subsequent authentications should then be continuous and the least intrusive as possible. As a result, will this foster convergence between Identification and authentication?

Reverification is the target because that is where the market wants to move. Banks don't want to move there but regulators are pushing them to re-KYC every 3-5 years depending on the customer's risk profile.

The question is not how many times a customer must verify, but how can we eliminate friction from each instance. It's about completing a proper identification once and then reusing that throughout the customer lifecycle.

In the end, the least number of times you can authenticate a customer is every transaction, as some

type of credential will be used, even if it is just unlocking their phone screen. The main question from a consumer's perspective is consent. We should aim for a process where authentication happens every time the user wants to be identified.

Continuous KYC represents AML needs, but it gets back to authentication. You don't have to show documents when we know it is you. We are clearly moving to a future where you can approve high-value transactions with your face.

Another important consideration is how many data controllers there are. Estonia has one, but the British have an aversion to one data controller, so we have to take into account cultural and regulatory values. To simplify authentication, we need locally compliant flows in different countries to accommodate different regulatory frameworks or user preferences.

Much of this depends on how governments define a strong ID, which is sometimes strong high-tech ID cards. An EU wallet and common identity will come and getting it right will be the most important task in light of what the FANG companies are doing. We need to find ways to help governments improve the strength of their identity systems.

Looking at Germany, for example, BaFin doesn't just want video KYC. Sometimes the live video call serves the purpose, which is much more secure than presenting a document at an office to a civil servant who is not trained to verify documents. When using a live agent, we have to remember that people are subjective by nature. Objectivity is achieved by database decisions and automation, which is why we want regulators to understand this better. Regulators push back on algorithmic bias and discrimination, but it's still better than humans are.

> Sometimes the obstacle is not the law as such, like GPDR, but the local authorities' understanding of that law, especially around the data and how to authenticate it.

WHAT ARE THE OBSTACLES?

Regulatory differences are not a genuine obstacle. The real obstacle is how to solve these regulatory differences for clients so one solution works for multiple countries. Said another way, can we make a seamless digital wallet that operates across markets and doesn't get killed by national barriers?

Regulatory differences certainly represent an opportunity for us to solve that complexity. Sometimes the obstacle is not the law as such, like GPDR, but the local authorities' understanding of that law, especially around the data and how to authenticate it. For example, in Estonia, if you request data validation, you would get it. However, in Romania, you would not get anything. Also, some countries expose their verification services securely to third parties so companies can check against their national strong identity. It's down to institutional understanding.

Does ID verification need to be solved by governments when many have proven they are not good at it? Governments should authorize an ID and audit 3-5 companies that distribute those IDs, rather than building and owning the ID infrastructures. For example, Europe's eIDAS (electronic IDentification, Authentication and trust Services) system is government-regulated but has a federated operation.

The BaFin rules prudently allow for asynchronous video recording, while the Swiss want you to localize security features. The Dutch regulators, meanwhile, are one of the first moving to biometrics.

Education for regulators is needed so they can learn and we can move the industry forward faster. Yes, we can automate, but we never say we need to remove all human involvement. Regulators will never accept a black box system, which means automation must be about increasing quality.

Speaking of automation, matching is the easy bit, but it's much harder to recognize a deepfake as liveness challenges are hard for humans to solve. There is a prejudice among regulators that the technology is flaky and humans will sort it out, whereas humans actually introduce noise into the equation.

Biometrics is a means to make subsequent authentications more frictionless, but it shouldn't come at the expense of privacy and security. We want to authenticate without storing data in a central database. Phone tokens verify as a second factor, but it's not great to have biometric data stored in a local place for a long time. We need a user-friendly way to continuously identify customers without having to ask for passports.

On a related note, Covid health certificates have changed the landscape for digital IDs and pan-European recognition. It proved governments can't solve the verification issue because we don't have one regional super app. Covid certificates are required at grocery stores, but stores still require a passport or other strong ID. They have become a box-ticking exercise and a colossal missed opportunity.

Biometric authentication of vaccination certainly raised an uproar, demonstrating how much biometric firms need to do more public education. We have a responsibility to talk to regulators about the opportunities and risks of biometrics as the best way to demonstrate identity.

VERIFIABLE CREDENTIALS

Verifiable credentials and zero-knowledge proofs are technologically quite interesting but there are still flaws. If you go through the process of ID verification, we should empower citizens to control how their data is shared. Zero-knowledge proofs are good, but does technology always improve the status quo?

Moving from a centralized ID scheme or fragmented IDs to something that is user-centric is a great way to go, but it is only useful once there is a marketplace for ID verifiers, holders, and users.

In a verifiable credential model, who is the data controller, as the data will be on the customer side? The first principle is an individual's national ID, so there will still be an onboarding process. In 5-10 years, businesses will be onboarding people to their verifiable credentials and authenticating them to those.

There is real demand for self-serve IDs, but who will pay for the infrastructure? There may be scenarios where merchants could pay for the service. For example, if a supermarket introduces a verifiable credential into your Apple wallet, they will be able to authenticate alcohol purchases. That said, some consumers may want to pay for it because it will be so much cheaper than the inefficiency of re-authenticating for each transaction. Also, the cost savings in reusing the information may encourage banks to pay for it. Electricity grid infrastructure, which is paid for by the operators, could be another model. Banks, who save money from the new infrastructure, would act as the grid operators.

In Estonia, the government made the digital ID cheaper than the passport, wrote it into law that you need an ID, and then lobbied the banks that they needed this for account opening. Similarly, we will need to build up a network of businesses to utilize verifiable credentials once the market is ready.

Until they have sorted out how verifiable credentials will work under GDPR, the European Commission doesn't want the consumer to be the data controller. However, under GDPR, individuals are the controller. For national governments, the problem is that they realize they can make money off of this.

> Banks, who save money from the new infrastructure, would act as the [electricity] grid operators.

WHAT SHOULD EIDAS BECOME?

Governments should create the infrastructure and framework and leave the market to attract customers by solving problems. For example, Europe's eIDAS needs to be clearer across jurisdictions.

eIDAS says ID verification should be the same strength as a physical ID. Meanwhile, in the Netherlands, the law around digital government has been sitting in parliament for two years. eIDAS should solve this today, but in practice, it has not.

Assessments of what constitutes strong verification in each country follow different criteria, but eIDAS only tells you the methods of testing, not the thresholds for passing those tests. The European Commission should define those conditions and not allow auditors to operate differently.

Opening up ID wallets to third parties to create a competitive market for services is not that bad of a base to begin from. A European ID wallet will be as important as the Euro was to the Union.

Contact

CONTENT:

Gary Dempsey
gary@money2020.com

Elena Mesropyan
elena@money2020.com

SPONSORSHIP:

Rachel Martin
rachel.martin@ascential.com

europe.money2020.com