Regulated crypto or Crypto Regulation?

Dive into digital asset trends & associated risks and regulations

A series that combines the views and insights of DLT/blockchain, digital asset, risk, and compliance experts

Volume 1

presented by SyntiFi

2023

SyntiFi
Next generation risk intelligence

Imprint

Title:	Regulated crypto or Crypto regulation?
Contributors:	Remo Stieger, Co-Founder & Partner, SyntiFi GmbH Viola Zoller, Community & Ecosystem, SyntiFi GmbH
Paper edit and design:	Viola Zoller
Institution:	SyntiFi GmbH, Baarerstrasse 10, 6300 Zug, Switzerland, info@syntifi.com
Industry Experts	Mark Greenslade, Casper Association, Switzerland Andrew Wishart, SIX Digital Exchange (SDX), Switzerland Tim Hall, University of Winchester, United Kingdom
Paper series:	Volume 1
Year:	2023
Location:	Zug, Switzerland

Preface

Decentralized Finance will never deliver on its potential as long as systems that allow market players to commit financial crimes, fund terrorism or launder money are allowed to propagate. Ensuring a compliant, righteous, and safe environment for blockchain-based systems and transactions is the responsibility of all participants in a decentralized system. This brings several challenges to applications and users alike, in particular in the areas of (1) privacy and (2) identity/digital credentials.

The question of "who I am" is answered by identity. Authentication on the other hand addresses the question of "proving that I am what I claim to be". In the physical world, people's identity is authenticated by e.g. ID/Passports and bank cards while in the digital world an indirect authentication applies through trusted institutions which file data with central authorities e.g. using mobile numbers or social accounts. Both worlds ultimately depend on trusted centralized institutions and services which collect users' private identity data.

To protect an economy from bad actors, one need to ensure that participants and assets are "clean". Self-custody, as one of the main advantages of blockchain, increases decentralization but comes at a cost of accountability and responsibility. Government regulations intend to keep us safe but come at the cost of privacy. AML and KYC/KYB play distinct roles at distinct stages of the customer journey, but both are of paramount importance for an integrated approach to compliance and financial crime prevention.

In this paper (volume 1) we discuss how industry experts assess specific risks from crypto asset activity and how they weave in vulnerabilities into their evaluation of risk in a business context.

Remo Stieger

About SyntiFi

SyntiFi GmbH enables financial institutions to interact with businesses that transact on the blockchain and meet compliance as well as regulatory requirements.

Originated and based in Switzerland, we offer effective technology solutions and new innovative methods of on-chain risk monitoring, data analysis, visualization, digital asset compliance and actionable blockchain intelligence to protect the integrity of digital asset transactions and to manage its risks, thereby strengthening efforts to prevent money laundering, fight fraud and stop financial crime.

Since launching in 2021, we have been on a mission to disrupt financially motivated crime across blockchain based and traditional finance industries. In that time, we have grown into a team defined by team spirit, collaboration and commitment to improving the status quo and to achieve simultaneously objectives for privacy, safety and financial inclusion. Our team consist of experts in Technology, Legal/Compliance and Financial Markets with a proven track record of driving digital transformation in tech and financial services.

Remo Stieger

Co-Founder and Partner I

SyntiFi

www.linkedin.com/in/remostieger/

Content

Industry Experts Portrait: Mark Greenslade

Mark Greenslade

Head of Research and Development (R&D) I

Casper Association, Zug

www.linkedin.com/in/mark-greenslade/

Mark Greenslade is a full stack, clean-code, polyglot technologist with deep open-source agile exposure. Highly experienced in delivering coherent solutions to complex systems for private & public sector entities across Europe & beyond. A genuinely strategic thinker who brings to the table a rare combination of analytical & creative skills. Urbane, values driven, authentic, sociable & at ease creating the space for teams to flourish. Chair of the IEEE (CH) Working Group on Decentralised Systems. Member of the Central Bank Research Association. Comfortable at the bleeding edge of R&D.

What is Casper Blockchain network and what are your current research topics?

Mark Greenslade: Casper is a Layer 1 Blockchain network, meaning that a network of computers (called nodes) run the Casper Blockchain software. Part of the software design implementation has a cryptocurrency associated with it, which is used to secure the network - it essentially functions as a security guarantee. To run a node on this network, one can either simply spin up a respective device and run the software as it is or participate in a competitive process (called auction) to get an elevated authorization with the right to validate blocks. Validators who successfully go through an auction process and subsequently become a member of a validator set, are entitled to propose blocks in which transactions dispatched into the network get organized in for execution. Consequently, these validator sets operate the consensus mechanism and subsequently drive the chain forward in response to the transactions dispatched by the end users, which may be DApps, individuals, institutions, etc.

One topic - and an always ongoing process - is strengthening the security guarantees around the consensus mechanism: If there is any compromise of the consensus mechanism, then the network will fragment and fold. Another area of research is how the present platform could potentially be modularized: Currently, the Casper network is classified as a monolithic Layer 1 Blockchain network, which means that all nodes have to execute all transactions and store all the data – and that's not optimal. We are exploring options to progressively modularize the platform, so that not all nodes need to execute all transactions and store all the data, which would reduce the computational as well as the memory footprint of the network.

A unique topic we are working on at the Casper R&D team is that we use ACTUS (Algorithmic Financial Contract Standard), an emerging financial standard, as a focalizing use case. Consequently, we ask ourselves how we can responsibly and securely serve the whole lifecycle of financial contracts leveraging this standard and which infrastructure we need to provide to achieve that.

Industry Experts Portrait: Andrew Wishart

Andrew Wishart

SDX Web 3 Sales & Relationships Global I

SIX Digital Exchange (SDX), Zürich

www.linkedin.com/in/andrew-wishart-243a3412/

Andrew Wishart joined SDX in September 2019 as Senior Client Relationship Manager. Andrew is an entrepreneur & finance professional with 14 years of experience in the Financial Services Industry and five years of running a successful multi-award-winning start-up business in Melbourne, Australia.

As a key senior sales and business developer at SDX, Andrew brought some of the first banks onboard to SDX and educated the broader market on the SIX Digital Exchange proposition. Andrew's current focus is on Digital Asset strategies, institutional crypto adoption & elements of DeFi in the institutional space.

Prior to SDX, Andrew worked at UBS for seven years in various Management roles applying new and digital technologies to help service emerging client needs.

How is the blockchain technology used at SDX (applications)?

Andrew Wishart: At SDX, the SDX Digital Securities division and the SDX Web3 Services use DLT/ blockchain technology differently and separately. For the former, SDX runs a permissioned DLT network. The reason for this is that back in 2018 - when we started - public blockchains were not mature enough to run financial market infrastructure (FMI). In the SDX permissioned DLT network, the consensus mechanism in that sense is SDX (i.e., SDX is the notary node), and this for example permissions participants into the network and ensures that there is no double spending. The assets are tokenised native digital securities—currently equity products and debt instruments—and we are looking into expanding the asset classes. The lifecycle aspects of these assets are managed through smart contracts—some fully automated, some semi-automated. We additionally have–and this is our unique value proposition–commercial bank money on chain (e.g., Swiss Franc and Euro in tokenized form, in other words digital money), as a means of settlement in the network.

For the Web3 Services, we work together with a company called Fireblocks to access various public blockchains, currently 39 protocols. We have an on-prem version of Fireblocks, which is quite a unique setup. For the staking services, we also facilitate the access for our clients. Hence, as a conclusion, at this point in time, we ourselves do not run directly on a blockchain, we rather orchestrate access to public blockchains and specialise in the security infrastructure around that including securely safeguarding the private keys for our clients.

Industry Experts Portrait: Tim Hall

Tim Hall

Professor of Interdisciplinary Social Studies I University of Winchester, Department of Policing, Criminology and Forensics, UK

www.linkedin.com/in/tim-hall-b605a6225/

Tim Hall is Professor of Interdisciplinary Social Studies at the University of Winchester. He is a criminologist and human geographer with interests in crime and globalisation. Tim Hall's ongoing research is unified by an interest in the spatial aspects of illicit and illegal practices. These, he examines largely through the lens of economic geography, This research includes practices such as organised crime and cybercrime and the regulatory responses to these. He has looked particularly at the significance of criminal organisations in the contemporary global economy and has published extensively in these fields and presented the results of his research at a number of international conferences. His recent research has focused on the geographies of economic cybercrime and explored the factors that cause cybercrime to develop extensively in certain parts of the world.

Tim is the author of a number of books including The Economic Geographies of Organized Crime (Guilford, 2018) and the co-editor of books including The Illicit and Illegal in Regional and Urban Governance and Development: Corrupt Places (Routledge, 2017, with Francesco Chiodelli and Ray Hudson) and A Research Agenda for Global Crime (Edward Elgar, 2019 with Vincenzo Scalia).

How, when, and why did you start engaging in the field of criminology?

Tim Hall: I probably started looking into this field 15 or 16 years ago. My background, however, is in Geography – which is very different to what I am doing now. I obtained a Bachelor's degree in Geography and a PhD in Urban Geography and then started teaching, among other courses, Economic Geography. Through that I became really interested in the geography of illegal economic activities and started to integrate modules about crime schemes and their distribution around the world into my teaching. In parallel, I realized that topics around organized crime haven't been much looked at from a geography point of view – which sparked my interest to also do research in that field. I published a number of papers, which were very well received: The last 12 years about organized crime in general and more recently about cybercrime, mainly financial crime, from a geographical point of view. So that's how I've got into that.

Opportunities & Challenges

Advantages in cryptography and digitalization have led to the development of financial innovation. With an estimated market capitalization of about USD 1.2 trillion as of H1 of 2023, digital assets became an important part of the financial industry.[1]

1 Source: www.coinmarketcap.com

1.1 In your opinion, what are the opportunities of Blockchain technology?

Tim Hall: I think the opportunities are huge. These new technologies are part of what is referred to as the 4th Industrial Revolution and have hence the potential to transform all kind of aspects of our work environment and ways of working and subsequently the economy as well as society. I see this as the latest wave in a series of historical waves of innovation and each one of those led to huge changes in particular industries.

Historically, such transformative innovations brought a lot of opportunities, but I believe that we have not yet fully understood what they might be in this case and also what the potential challenges are – I think we are a few years away from that.

Nonetheless, I truly believe that we are in the middle of a profound economic transformation with these new technologies spurring the next cycle of global economic innovation and growth.

In terms of the Blockchain technology, it seems to have gone from being a niche and specialized technology to become one that people are much more aware of and being used much more widely nowadays.

Andrew Wishart: In my opinion, what is critical for this new era of FMI is the fact that "the value" and "the technology" have converged in form of token economic business models: This effectively allows a much freer way to transact value—which I think is the fundamental benefit that is brought in.

And secondary to that—given that the value is embedded within the technology–the value can be programmed directly rather than indirectly as it was done before, which provides a direct and final way of how these token economic business models can operate.

Mark Greenslade: From an institutional perspective what is needed in terms of Blockchain, which results in opportunities, I can say that the number one requirement is that institutions are able to examine the user's commitment to a transaction and whether the network has executed the transaction as intended by the user. Hence, the network must be able to provide proof that both commitment and transaction content were respected by the infrastructure, for example through audit trails of transactions and signature records.

Further, the infrastructure should provide real-time - or at least very near time - observation mechanics to, e.g., track and trace transactions as well as account activities. The reason for it is that in this system where blocks are being executed within certain time intervals, there is always a time gap between the moment a transaction request is dispatched into the network and the moment it gets executed. During this time gap, attack patterns can be executed by malicious actors. So, the blockchain infrastructure needs to allow a high degree of observability, as this otherwise may become problematic.

It is however not necessarily the blockchain itself that would provide these observation mechanisms, but rather ecosystem tools and SDKs around it.

Also, the core engineering teams of blockchains are generally system programmers heavily involved in consensus concerns and less in business requirements from companies interacting with the blockchain.
That's why entities like SyntiFi are so important to any blockchain network, as these kinds of entities are needed to build up this higher order transaction and account profiling infrastructure.

1.2 And what are the challenges?

Tim Hall: I think there are general challenges as well as specific ones related to the use of these new technologies by criminal actors.
The general challenges are those anxieties that people are expressing now towards these new technologies, especially about their impact on their jobs – which is a phenomenon that can be observed for all transformative technologies. I think it's a genuine concern, as it is certain that these technologies will transform jobs. Also, for this point I believe we are at a point where we don't know exactly how this will work out.
In terms of specific challenges linked to the use by criminals, all come back to the fact that criminals, especially the ones involved in any form of technological crime or cybercrime, are incredibly innovative. For example, I am hearing anecdotes about criminals using AI to generate fraud scripts, which they previously had to write themselves.
So, there are specific challenges linked to how malicious actors might use these new technologies, but again, I believe this is just emerging and we do not see all the impacts yet.

Andrew Wishart: I think the challenges on the business side and the technological challenges are–at least partly–interlinked. The business side is fundamentally challenged by the regulatory unclarity around the technology and its applications.
In Switzerland, there is a framework around digital assets—the DLT law—which however applies more to public blockchain issued securities and less, for example, to cryptocurrencies: They are a global phenomenon and not a jurisdictional asset class and are hence treated differently in different jurisdictions.
So, as one can already see from this example, there is uncertainty around dealing with the technology and these on chain assets.
SDX is a regulated FMI in close contact with FINMA and wants to make sure that the trust that was built up sustains, thus we move at the appropriate pace to make sure that we incorporate all the necessary checks and balances.
However, that then in turn poses business challenges on how quickly we can move.

Mark Greenslade: One challenge is social and that is keeping engineering teams intact – to deliver world-class software, one needs a world-class team. Achieving this includes creating an environment in which these teams can focus without being distracted and a healthy and fun environment for them to flourish.
Another challenge is to provide appropriate testing infrastructure, and I believe it's frequently underestimated how important and complex that actually is: Rolling out major upgrades on a permissionless blockchain is not easy and involves a lot of risks. Consequently, upgrades must be tested extensively before the roll-out.
The public test networks are useful mechanisms to do that before entering a production network. However, before you get anywhere near a public test network, a series of private integration tests have to be done – and this significant engineering infrastructure is often underestimated.

Key risks from business and tech perspective

The importance of understanding the risks posed by innovative technology and markets has been highlighted by various events in the past which caused financial instability. Identifying these risks and analysing their implications enable prevention and timely mitigation.

2.1 What are the risks related to digital asset/blockchain transactions?

Andrew Wishart: One key risk is that you may lose the key, say access, to your digital assets—the ownership of the asset being in your control comes with a responsibility.

Our ethos is that once you start transferring significant amounts of value, you do not want to expose yourself to that particular risk. In my view, not every institution wants to manage the access rights themselves.

Mark Greenslade: To determine the risks related to transactions the questions that needs to be answered are: Who is transacting?; What are the risk profiles associated with any involved parties according to KYC processes and AML requirements?; How are they transacting and what are the associated counter party risk?

Further, in a system where transactions are placed by the users and then distributed through the network, those transactions become visible - not necessarily the identities of the involved parties, but the queue of transactions as well as transaction details can be viewed in advance of execution.

The problem that this brings on the table is that depending on the type of transaction there might be "attacks" – I say it within quotation marks, because they are neither due to protocol failures nor operational cheating, but simply possible because of the described nature of the system.

One example for this is a 'sandwich attack'. In this attack, malicious parties scan the queue of transactions and then strategically inject transactions before and after a waiting transaction (hence sandwich), resulting in that the system does not process the transaction as originally intended, in other words the integrity of the intent of the transaction is violated.

Here comes the so-called intent-centric architecture into play. Until recently I thought that this is just another buzzword, however this really concerns the question whether the system will execute the transaction or any other action that a user intends faithfully. Intent-centric systems really try to stay faithful to the original intent of the transactee – and this idea is entering the system architecture designs more and more.

2.2. How do these risks impact the adoption of digital assets / the blockchain ecosystem in general?

Andrew Wishart: I think it is playing a big part, because there are various blockchain protocols and they work very differently. So, to be able to manage those, to provide access to those and to secure the keys associated to those can be quite individual and some may even require a setup with a master key and subkeys. Thus, the whole topic is not trivial and requires an appropriate operational setup, including governance and segregation of duties, which subsequently generates costs.

One example for this being not done properly was the case of FTX. Its collapse had nothing to do with the technology, but the way the company was operating; how the company was being audited; the misuse of customer funds; absent segregation of duties; key people risks, etc.

Box 1:

Legacy infrastructure systems vs blockchain infrastructure: What are the similarities, but also differences, as well as the pros & cons of each system?

Mark Greenslade: The existing systems are very successful: They have scaled, they are relatively secure, and there are a lot of standards around compliance and regulations for these systems. Their primary disadvantage is that they are fairly closed systems with strong access control mechanics and "centralised" authorities. Trying to interact with the SWIFT network is a good example: it's quite difficult to onboard in that network and to become a SWIFT partner. On the other hand, in closed environments dispute mechanisms and system failure protocols exist and jurisdictional anchoring is given. This is crucial when running financial infrastructure, as these measures are in place to mitigate the risks of the network participants and also to increase financial stability as a whole.

Permissionless blockchain environments are open, which is their strength. However, because they are open, it's a highly hostile space, in the sense that if someone sees an opportunity to compromise or exploit the network they will do so. So, just the fact that these systems are surviving in this hostile environment is a strong signal that they are here to stay: They have proven themselves resilient and robust to a certain degree. Having said that, blockchain networks are being exploited almost every day, and it's not just the base layer, such as the Casper chain that can be corrupted or successfully attacked, but also the 2nd and 3rd layers on top of the base layer. Further, in case of a consensus failure, there is the option of hard forking, however this is a controversial strategy as it goes against the notion of immutability and censorship. But I think one needs to take a holistic view and recognise that the value should not be compromised simply because of operational failure at protocol level.

To summarize, imagine a spectrum where you have on one side open and adaptive systems and on the other closed and static ones. In an evolutionary context, the former typically out wins the latter and I think that this is probably also true for how the blockchain space could over a period of time really provide an advantage.

Money laundering & financial crime

While digital assets become more widely used, an alternative financial system may be created. Not only new forms of financial crimes are resulting, but in particular the connection with the fiscal, real and traditional financial industry may pose a significant risk to the financial stability.

3.1 Do digital asset / blockchain transactions enable money laundering?

Andrew Wishart: A few years back, people were talking about Bitcoins being used on the Silkroad to purchase illicit drugs and weapons, and this got Bitcoin—and cryptocurrencies in general—a negative reputation. There are cryptocurrencies that are designed in a way that the ownership and some of the money flow components can be obscured, which makes it more difficult to track them and thus might enable illicit transactions.

Cryptocurrencies are however only one subcategory of the broader category of digital assets.

At SDX, we developed a token framework concerning which protocols, and subsequently which cryptocurrencies, we want to cover or offer. For example, in order to be accepted, a protocol needs to be transparent to the extent that we can trace the coins and ultimately feel comfortable to take these assets into our custody. On the digital asset side as such, where we deal with actual securities, they must effectively adhere to the same rule book and hence go through the same checks as traditional assets.

So that's how SDX distinguishes between dealing with traditional assets in digital form and with cryptocurrencies, whereas some nuances apply to the latter depending on the protocol.

Mark Greenslade: In permissionless networks basically everyone can setup a wallet very easily. Then the wallet gets funded through either fiat on-ramping or someone in the 'laundering chain' sending funds to that wallet – and just like that the wallet is ready to be used to wash illicit funds. So, it is simple to set up money laundering activities on-chain.

Also, the absence of in-build KYC processes and AML mechanisms makes digital asset ecosystems more attractive for money laundering than mainstream financial infrastructure, where both are present. Indeed, various money laundering cases were uncovered in which state and non-state actors used on-chain systems to launder the proceeds of illicit activities and then withdraw them into fiat. However, to scale money laundering operations, malicious actors will opt for wherever the liquidity is the highest and that is in the latter.

So, to summarize, the cryptocurrency space is attractive for money laundering activities, because its permissionless, but it's done at a fairly small scale.

Tim Hall: The first thing to say is that cryptocurrencies are indeed used in criminal activities and to launder money – there is plenty of evidence for that.

The pseudo-anonymous nature of cryptocurrencies is

beneficial for money launderer to disguise the origins of funds. Further, cryptocurrencies potentially allow money laundering at a larger scale than in pre-digital ages, when criminals literally had to handle a bunch of cash and launder it for example through racecourses, which took a long time to do.

However, I think it's unfair to blame the blockchain technology and cryptocurrencies as the cause of such activities – as it is frequently done. I'd rather say they are part – and currently the latest phase - of a global digital financial infrastructure that has been evolving over the last few decades that facilitates money laundering at a larger scale. Hence, they should not be blamed to cause a sudden appearance of something that wasn't there before, it's an evolution of a longer-term trend.

3.2 Can blockchain technology potentially be used to stop financial crime?

Andrew Wishart: Yes, I think it potentially can. Every transaction is casted to the network and recorded in an open ledger and is thus transparent. Through that, a lot of data is being built up and mapped out.

So, provided that the relevant parties have the capabilities to identify and track transactions, financial crime might be detected. Indeed, there are blockchain forensic tools that are used by (inter-)governmental agencies to track (financial) crimes.

Mark Greenslade: I believe that for the blockchain ecosystems to start scaling beyond where they are at the moment, including attracting more capital and different types of assets, and for the space to make a step forward in terms of maturity, these concerns should be taken more seriously by the ecosystem participants and not just getting hand waved.

For instance, base layer protocols should provide opt-in mechanisms for KYC & AML mechanism at the account level. I have proposed this within the Casper project, even before it went to Mainnet. But you get resistance, because there is an ideological commitment that the Platform should be permissionless - but my question is then at what price and social responsibility?

Further, in my opinion, there should be more horizontal coordination amongst the blockchain foundations with the aim to develop a common approach towards KYC & AML requirements– I don't see a lot of talks or working groups amongst the blockchain foundations in this area. However, I think this would be crucial.

Tim Hall: I think there is extensive potential for that. A blockchain records every transaction and subsequently a permanent record of every transaction linked to a specific digital asset is available. This potentially creates far more transparency than ever before. I like to use the following analogy: It's like having a 50-pound bill that has the name of every person whose hands it went through written on it. The presence of that kind of information is potentially hugely valuable.

As always though, there are challenges. One of them being that at the moment the sharing of this kind of information and data is restricted by commercial sensitivities and reputational issues. So, I think the challenge is to find a suitable way to use and share them. Hence, companies, like SyntiFi that flag and help to understand risks are really important.

Also in an academic sense, the data could be used for analysis to understand criminal patterns better and to identify where and how cryptocurrencies, NFTs and other crypto-based assets are used for illicit activities.

There is a whole range of potential avenues. First of all, technical cybersecurity is very important, especially for countries that see a rapid increase in computer usage—as the cybersecurity dimension often lags behind, that makes people easy targets.

When looking at the cyber-criminogenic framework (Box 2), specific factors identified with the support of this framework can inform the policymaking of governments and point towards potential risks, especially when designing policies to promote their national IT sector and IT education.

Another strategy is to try to identify potential future cybercrime hubs to be able to implement risk measures in an timely fashion. Currently, I am working on a statistical analysis whereby the impact of future economic scenarios, for example a global recession, on cybercrime activities are analyzed.

3.3 A main advantage of blockchain is cryptographic secured self-custody of funds, meaning there is no need for a "middelman" such as financial institution to manage the funds. How do you assess this development from a criminology point of view?

Tim Hall: In theory, not having to use financial institutions as a middleman is a positive aspect for criminals, as it limits their exposure to scrutiny to a certain extent and it's probably one of the reasons why they are using cryptocurrencies. However, looking closer at the role banks and other financial institutions played in the past in detecting and preventing money laundering, it is important to acknowledge that various instances have exposed them as not being very willing or efficient in unveiling money laundering activities or flagging illicit funds that were passing through them. Indeed, there have been cases of large international banks being fined millions of dollars for failing to scrutinize fund flows from and to them.

So, as a summary, while cutting out banks and other financial institutions can be beneficial for criminals, we should not assume that the financial sector has been particularly effective so far in preventing money laundering.

Box 2:

What roles do geographies play with regards to financial crime?

Tim Hall: The first thing to say is that in theory one can commit cybercrimes from anywhere in the world as long as internet connectivity is given. In fact, many people think that cybercrime is a universal threat that can come from anywhere. However, there are strong regional concentrations of cybercrime activities, in particular in West Africa in Nigeria, Ghana, and Ivory Coast, in Eastern Europe in Romania and Georgia, and to a certain extent also in Türkiye and Brazil. Similarly, highly concentrated cybercrime clusters can be identified within these countries. For example, there are specific cities in Romania where thousands of people work for the local cybercrime industry committing fraud. Hence, I focused my research on the question of why there are these concentrations of cybercrime in certain geographical areas. To achieve this, I went through numerous accounts of cybercrimes to identify the conditions that exist in high-cybercrime countries or regions that drive cybercrime, with the understanding that cybercrime is a product of certain conditions coming together within these places. I summarized my findings in the cyber-criminogenic framework.

In a nutshell, the regional cyber-criminogenic framework is an attempt to bring together all the potential factors or conditions that might contribute to cybercrime – criminogenic basically means "causing crime". As outlined previously, I analyzed cybercrime accounts from different regions to identify the factors or conditions that are contributing to cybercrime in that specific context – it was and still is quite an explorative work.

One finding is that there are a wide range of such factors. The two that came out most strongly though are IT literacy in association with regional poverty, meaning where you have a combination of these two factors, cybercrime is generally quite prevalent. Other relevant factors are social and cultural. For example, cybercrime rates are higher in countries where cybercrime enjoys some sort of social legitimacy or is seen as less criminal than other forms of crime and in cultures that are materialistic and wealth accumulation is highly valued by society.

(continues on page 15)

Box 2 (continued):

Additionally, political factors can also be identified. For instance, in Nigeria, citizens can observe obvious cases of corruption by politicians, which they use then as a kind of justification for their own illicit activities.
Or if you take the example of China, a geopolitical dimension can be observed there: Being a cybercriminal is seen as something patriotic as they target enemies – say other countries - and hence the state does not see the necessity to prosecute them. A last factor that I am mentioning here is the chance of cybercriminals being caught and convicted: In high cybercrime countries, and particularly in Africa, the cybercrime policing is generally limited by scarce resources. These are just a few out of the many identified factors.
What is needed now in a second step is a more systematic analysis of that framework to, for example, identify how these factors apply to different forms of economic cybercrimes and whether some factors apply in some regions, but not in others.

You wrote a paper about the case of Armenia. What is the relationship between IT development, regional poverty, and cybercrime and how can the outcome of your research be applied to other regions?

Tim Hall: Armenia is an interesting case. A colleague and I started this project three years ago and we approached our research by expecting that Armenia will be a country with a high amount of cybercrime. Not a lot has been written about Armenia in the cybercrime literature, but the conditions for a high-cybercrime country are present: Armenia is a post-Soviet country with high regional poverty and a government pursuing a strategy of IT development and IT education over the last 20 years – and those are some of the conditions that often lead to high levels of cybercrime. An example for that is Nigeria, famous for its email-phishing scams and now more recently romance scams: In Nigeria numerous very computer literate graduates cannot find jobs in the legit economy, due to a lack of availability of such jobs and subsequently opt for cybercrime. We were expecting to see something similar in Armenia, but what we actually found was that there is relatively little cybercrime in Armenia. Reasons for that are manifold. First of all, Armenia's legitimate IT sector has grown incredibly rapidly in recent years and is hence able to absorb the IT-literate graduates and provide them with jobs that are well paid and enable a good middleclass lifestyle. Armenia's IT sector is mainly so successful and growing because the country's large diaspora community invested heavily in their home country, for example, by opening or expanding companies in Armenia. Another reason for the low cybercrime rate is cultural: In Armenia, younger generations distant themselves from the old ideas of corruption and crime that are linked to previous generations and regimes and see crime in negative terms.
The second part of the question, i.e. how one can apply the findings from Armenia to other countries, is interesting. One main finding of my research is that there are concerns that policies promoting IT education might have the unintended consequence of leading to an increase in cybercrime activities. So, the fundamental lesson from Armenia is that governments can promote IT developments in the context of regional poverty without leading to cybercrime. The challenge is though, to replicate what happened in Armenia elsewhere – Armenia is definitely an unusual case. Another success case is Rwanda: The country has established itself as a digital hub, without the side effect of increasing cybercrime activities.

Regulations

The regulation and supervision of digital assets pose challenges as innovation comes along with complex systems and environments. Legal and regulatory risks could quickly increase leading to a need of legislative initiatives which address new risks but also support innovation and work hand in hand with current regulatory practices.

4.1 What is your assessment of the current blockchain/digital asset regulations?

Andrew Wishart: In my opinion, Switzerland has done a really good job in creating its regulatory clarity around digital assets. It has also opened the playing field for different players to engage in this new way of transacting securities.

However, I think one of the remaining challenges is that a critical mass is needed to be able to fully transition to digital assets for the various asset classes. The way the financial market industry has developed and the complex structures around funds, private markets, special funds vehicles, etc. create a myriad of challenges when switching to a digital asset landscape. I think that the regulator can further support this in part.

Also, the SDX Digital Securities business faces the challenge to reach a critical mass of adoption. SDX connected to the traditional sphere to support the ecosystem with the adoption and to thin the wall between the two.

New things will bring up new regulatory challenges and regulation always lacks behind. So, this journey will be a long one for everyone involved.

Mark Greenslade: Switzerland has been on the forefront and its regulations for the space are mature. This was achieved by paying attention to the needs of the involved stakeholders, taking into account the global dimension of the crypto-space and consistently following the chosen regulatory approach.

The blockchain and digital asset regulations are also getting more sophisticated, e.g., the list of available licences has been extended. Further, the dialogue between the regulator and industry players is well established.

I know that companies active in the digital asset space in Switzerland have a major advantage in comparison to their counterparties in other jurisdictions, because of the regulatory environment.

Tim Hall: I am not that familiar with them, but my understanding is that they are emerging. The challenge though, as always, is that the criminals are a bit ahead of the regulations – regulations are generally reactive.

In general I think regulations are hugely important, but also a real challenge. What I have seen in my research is that organized crime is benefitting from the fact that regulations are different in different parts of the world and malicious actors are constantly exploiting regulatory loopholes – and I think the same applies to cybercriminals.

For example, they may use servers and other IT infrastructure in parts of the world where regulations are not as stringent.

So, the easy theoretical answer is that regulating the

internet, financial instruments, cryptocurrencies and so on, is crucial to prevent financial cybercrime. However, achieving universal regulations is almost impossible, regardless of how desirable they would be. There is, for example, the Budapest Convention on Cybercrime that various countries have signed, but it's not enough.

I definitely encourage bringing cryptocurrencies and digital assets under existing AML legislation. But I think it's an illusion to assume that this will solve all the problems, as I believe there will always be regulatory loopholes that criminals will exploit.

4.2 What are the challenges when implementing the regulatory requirements that are attached to the FINMA license?

Andrew Wishart: We were posed at the beginning with a few choices around which licence to acquire for the SDX Digital Securities division. We decided to acquire a traditional licence and so in terms of regulatory challenges, the "same asset, same rules, same laws" principle applies. That's also why SDX built the infrastructure in such a way as to reflect traditional market structures.

Now, we cannot predict the future: Will there be new regulations? Will there be new ways of operating FMIs in the future? Which chain will all be working on? Which jurisdictions will adopt how? etc. These are all questions that one has to move with.

But those changes will come and there will probably be a lot of them between now and when we have a mature FMI on chain.

4.3 Should the blockchain technology/ digital assets be regulated to a greater extend?

Andrew Wishart: This is actually a difficult question. The whole premise, that brought the blockchain technology—or at least Bitcoin—more to the mainstream attention was the idea to create an internet money, a freer way of money, a different form of money.

The question is now whether this has been achieved yet. The nucleus of it is Bitcoin, but is Bitcoin itself money? Certainly not all the time and a lot of people would argue that it isn't money, but a very good store for value in a digital form. So, regulating this new flow of money—or value—is extremely challenging.

For example, some of the digital currencies are global, so they represent some forms of value to the holders in different jurisdictions, different tax systems, different cultures, different access to financial systems. Now, one extreme stance is to let it take its course, which goes in the direction what the US did, as they didn't find any regulatory clarity in dealing with it other than forbidding it in some parts, which then resulted in company like FTX going to the Bahamas.

Thus, in my view, one cannot ignore regulating blockchain as it transacts value, but how to regulate it is the one-billion-dollar question—and I believe a balanced framework is needed.

Additionally, I also think it's not just about regulating, but rather about organising a system that is fair: As Eric Vorhees always says "the code is law", so if you manage to embed fair values into the blockchain system, parts—not all of it—can be accomplished through fair code and that's probably the way to look at it, to deal with the challenges around the regulatory landscape in blockchain.

Outlook

Going forward, given the speed of innovation, progress and decentralization of the environment, addressing the significant risk and policy challenges with the right tools and infrastructure remains crucial while the digital asset market matures and becomes more integrated into the global economy.

5.1 How do you see the future of the blockchain technology and the crypto space?

Andrew Wishart: People are talking about tokenising everything; I believe that a lot more things will enter the space of value in which financial institutions and thus marketplaces will become interested in.

One example are gaming items that have value, are transacted, and require custody; another example is IP rights, and so for instance, what the next iteration of Spotify will be. Such things represent new types of value—or assets effectively—that are going to be transacted through different channels, across different countries, peer to peer or over marketplaces–some of them already exist in part today and others will be developed in the future. A lot of exciting developments are ahead.

In my opinion, the mainstream adoption of these types of values and accessing them will change to the extent that one will become much more used to using the technology, while at the same time the usability will be simplified.

Further, I believe that the access to the blockchain will in part be controlled—it won't be "utopian free wild world"; some areas might remain that way, but they will also be harder to access as a result of that.

When looking at the broader FMI space, I think that there will be a lot of friction taken out of the system and SDX wants to be part of that by enabling access to and mobilising liquidity for various asset classes that we believe we have a role to play in, such as traditional securities, but also new types of securities, including art and other collectibles.

It will ultimately be a client demand-driven decision to what areas the FMI spectrum expands out to, but certainly everything will be operating on chain.

Mark Greenslade: The crypto space has - and will have - to navigate challenges. For example, the SEC (United States Securities and Exchange Commission) is currently trying to get the industry under control, after it was not very forthcoming in regulating it.

I further think that the crypto space needs to take an honest look at itself and improve in how seriously it takes into account investor and consumer risks.

This goes in line with my observation that the FTX implosion was due to mismanagement, immaturity, and arrogance. In the same vein, if the space expects to attract public capital, such as pension funds, it should not complain about regulations, as everyone inside the industry knows how dubious the space can be.

I think that regulators are fully entitled to - and should be empowered to - set rules for this asset class. I like to use the following framework with the categories highly regulated, lightly regulated and not regulated: If you want these systems to operate in an unregulated environment, then you should accept the limitations of that, for example that public capital will not enter the space.

It's a bit different for private capital, as it is the private person's decision on how they want to invest their capital and how much risk they are willing to take.

Further, the blockchain landscape is undergoing a transformation from within, due to new forms of cryptographic techniques and their applications, either already or soon in production - and we at Casper are also looking into them. Of these new cryptographic techniques, the so-called zero-knowledge cryptography - a method to prove the validity of a statement without revealing the statement itself – probably gets the most attention, however there are also many others, such as secure multiparty computation and homomorphic encryption. They will collectively result in more secure custody setups and more secure transactions because there will be in-build guarantees to respect the details of the transactions.

I believe that we will see more and more Decentralised Exchanges (DEX) using these cryptographic primitives for dark pools where trading of financial contracts take place. Right now, in trading, all the traders can see each other, and their respective order flows and malicious actors may take advantage of that transparency. However, interacting with DEXs that are private by default and hence have only partly visible order books, is more attractive for trading, because the information leakage is reduced, and therefore the market function – and ultimately the market integrity – is sounder.

So, I believe that this will transform the digital asset landscape quite significantly: Those protocols that successfully implement this form of market mechanism and take governance and corporate responsibilities seriously will have a competitive advantage. As far as AML requirements are concerned though, this will certainly complicate supervision and compliance requirements in terms of transaction tracing and audit trails.

5.2 What are the latest trends in cybercrime?

Tim Hall: There are various trends in cybercrime. What I am beginning to think about more and more on is an aspect of cybercrime that has been overlooked in my opinion, namely domestic cybercrime.

Domestic cybercrime targets people in the same country as the cybercriminals are based. Evidence shows that domestic cybercrime is quite prevalent. There are reasons for opting for domestic rather than international cybercrime, such as the cybercriminals and victims speaking the same language and having the same cultural background. For example, I am becoming increasingly interested in domestic British cybercrime.

5.3 What might be future challenges for institutions, such as SDX – given the discussed future of technology and regulatory requirements?

Andre Wishart: We set out on a journey to position Switzerland, and the SIX group, as a pioneer in the digital asset space through providing access, driving liquidity into new use cases, and increasing the asset universe.

It hasn't been easy, but we have already achieved some of our goals and laid a foundation: we set up a functioning permissioned environment that is fully regulated and licenced; introduced on-chain settlement with commercial bank money; were part of CBDC experiments; established access to the world of public blockchains in a controlled way; and started offering validator services for key chains, like Ethereum.

The challenge is now to scale up and to expand the ecosystem with more members and customers. One way to achieve that is to install confidence in the traditional market space to bring more value into this new ecosystem, which is different from what they have been used to—and that requires support from our shareholders. At the same time, we keep innovating and coming up with new business models to support new types of digital asset classes.

So that's the journey we are on—we started it, so we will continue on it until we succeed!

About SyntiFi

SyntiFi GmbH enables financial institutions to interact with businesses that transact on the blockchain and meet compliance as well as regulatory requirements.

Originated and based in Switzerland, we offer effective technology solutions and new innovative methods of on-chain risk monitoring, data analysis, visualization, digital asset compliance and actionable blockchain intelligence to protect the integrity of digital asset transactions and to manage its risks, thereby strengthening efforts to prevent money laundering, fight fraud and stop financial crime.

Since launching in 2021, we have been on a mission to disrupt financially motivated crime across blockchain based and traditional finance industries. In that time, we have grown into a team defined by team spirit, collaboration and commitment to improving the status quo and to achieve simultaneously objectives for privacy, safety and financial inclusion. Our team consist of experts in Technology, Legal/Compliance and Financial Markets with a proven track record of driving digital transformation in tech and financial services.

Contact & further information

Email: info@syntifi.com
Website: www.syntifi.com
LinkedIn: company/syntifi
X (Twitter): @SyntiFi

SyntiFi
Next generation risk intelligence