Financial Technologies and Crime

Financial Technologies and Crime

An overview of the state of the art in research pertaining FinTech and its implications for crime

Borja Álvarez Martínez

PhD Student
Department of Criminology
The University of Manchester
borja.alvarez@postgrad.manchester.ac.uk

Table of Contents

Full citation: Álvarez Martínez, B. (2022). *Financial technologies and crime: An overview of the state of the art in research pertaining FinTech and its implications for crime*. Department of Criminology, University of Manchester.

This report maps the cutting edge of research in FinTech, with a focus on understanding its relationship with crime. To do so, we must keep in mind that this is an ecosystem which evolves extremely fast, involves the whole financial services sector, and is truly global in nature. The starting point to tackle this phenomenon was therefore exploring its different, sometimes competing, definitions, highlighting its conceptual problems. The report then explores how any technological revolution brings both advantages and increased operational vulnerabilities, which can be exploited for criminal purposes. It concludes that FinTech has either allowed for more efficient or complex ways of committing pre-existing offences or created new criminal opportunities altogether. As a result, research in FinTech is tackling four areas of interest for crime-oriented scholars and practitioners. These are fraud research, cybersecurity research, blockchain research, and money laundering research. Emphasis was put in the different data being used to investigate these phenomena, showcasing the pre-eminence of secondary data, and the nascent role of synthetic data. The report then moves to address the implications of the COVID-19 pandemic, and the contemporary Non-Fungible Tokens (NFTs) market craze. It then finalizes by addressing the need to further investigate key issues such as money laundering, user confidence, and an urgent need to better grasp the NFT phenomenon. This work is part of the CyberUp initiative, a project funded by the Research Collaboration Fund for Research Staff of the University of Manchester.

1. FinTech: A not-so-mature concept

Assessing what Financial Technologies, globally known as "FinTech", are, is in itself a complex task. Across disciplines, several definitions have emerged since the second half of the 2010 decade. FinTech is however not quite so novel a concept. It emerged in the early 90s, because of Citicorp's drive to create a common forum for financial services and technology corporations. This forum eventually coalesced into a research project named Fintech (Puschmann, 2017, Wójcik, 2021). Other authors even argue that early cases of FinTech go as far as the widespread usage of ATMs and the creation of SWIFT (Leong and Sung, 2018, Goldstein, Jiand and Karolyi, 2019). Nowadays, the term FinTech generally refers to either specific digital innovations (such as blockchain and cryptocurrencies) or technology-enabled business models within the financial sector (like P2P lending and mobile payment services) (Philippon, 2016, Allen, Gu and Jagtiani, 2020). However, given its ever increasing implementation, the term is still considered as volatile, insofar as the trend of applying advanced technological solutions to the financial sector is still being developed in new ways including big data analysis, machine learning and cloud computing applications, among many others (Gai, Qiu and Sun, 2018).

Because of its ambivalence, the term FinTech is applied in many contexts, but inconsistently and ambiguously, without practitioners agreeing to a common scientific meaning or practical common working definition (Schueffel, 2016). This has consequently led to a very weak public understanding of what FinTech is (Leong and Sung, 2018). After conducting an extensive literature review, Schueffel (2016) concluded that the only definition that can encompass all current phenomena associated to FinTech is that of a *"new financial industry that applies technology to improve financial activities"*. Given that the relevant factor is therefore the application of technology to solve specific financial issues, FinTech can be considered directly oriented to improve general operational efficiency (Philippon, 2016) and thus it is often developed to match pre-existing demand of the financial services (Gai, Qiu and Sun, 2018). A key feature is that this technological innovation is driven through start-up companies that deliver specific solutions to well-established banks and insurers (Puschmman, 2017). And therein precisely lies the uniqueness of the FinTech revolution: it is not being shaped only by the traditional actors in the financial industry, but rather by outsiders trying to disrupt the incumbents through start-ups and big technology firms (Goldstein, Jiand and Karolyi, 2019).

In short, as we can see from the different literatures, the definition of FinTech is very much a functionalist one. Whether a given application of technology constitutes or not FinTech appears to be a rather *post facto* affair, which makes difficult to ascertain whether cutting edge developments can be

considered as FinTech or not (such as blockchain, grey online markets and non-fungible tokens). Moreover, this approach is further problematized by the conceptual current that considers the Start-Up nature of the service provider to be a *sine qua non* requirement for a given technological implementation to be properly considered FinTech (see Puschman, 2017 and Goldstein, Jiand and Karolyi, 2019 for more detail on this debate). This creates clear ontological problems from a research perspective, as a given technological application might be considered FinTech for a certain time, and then, subject only to changes to its ownership, cease to be so. An example of this would be former London-based FinTech TransferWise (now operating as Wise), which after 10 years of operations was acquired by Visa Inc. As such, the same financial service would only be considered by some authors as FinTech when it was not owned by Visa, insofar as afterwards the Start-Up/SME requirement is no longer fulfilled. This furtherly blurs a concept which is not particularly clear-cut in the literature to begin with, and highlights the necessity of continuing the efforts towards a broad, comprehensive and inclusive definition that can be adequately operationalized for research, policy and regulatory purposes. The present status in which there is no agreement as to what FinTech entails (Schueffel, 2016) must be urgently overcome. However, it must be acknowledged that given the relative novelty, broad scope and hybrid nature of FinTech this undertaking is complex (Wójcik, 2021).

Regardless of the theoretical and conceptual discussion currently surrounding FinTech as a whole, substantive effort has been committed to map the benefits and drawbacks of the increasingly widespread adoption of these technologies across a wide variety of financial services (Allen, Gu and Jagtiani, 2020). As such, there is a wealth of literature from different disciplines within academia that are concerning themselves with mapping the implementation of FinTech in the current financial services industry, identifying its operational characteristics (see among others Philippon, 2016, Leong and Sung, 2018, Gai, Qiu and Sun, 2018, Allen, Gu and Jagtiani, 2020, Mehrban et al., 2020). This endeavour is being approached from a variety of disciplines (Geography, Information Systems, Management Studies or Computer Sciences, to name but a few), and its result are published throughout a variety of journals, some of which seem concerned with publishing special volumes gathering research about FinTech within their parochial scope of interest. For the purposes of giving a succinct overview of this ongoing discussion, in the following pages the proposed perceived benefits and drawbacks of current FinTechs will be examined.

1.1 A technological revolution? The benefits of FinTech

To fully grasp why FinTech, an inherently disruptive new framework (Schueffel, 2016), has penetrated all areas of the financial markets so quickly, it is fundamental to understand that it has *de facto* made

the overall system more efficient and capable (Allen, Gu and Jagtiani, 2020). The branches within this economic sector which have seen the most impact through business value creation are payments, advisory services and financing itself (Leong and Sung, 2018). Exactly which changes and potentialities FinTech has brought about in each of these subsectors will be discussed now:

a) ***Payment services:*** Within the payment sector itself FinTech has allowed the quick conversion of entire companies to a cashless model, through the development of in-house payment apps (Leong and Sung, 2018). Furthermore, FinTech has created, and indeed, delivered, the expectation of real-time payments (Philippon, 2016, Goldstein, Jiang and Karolyi, 2019, Allen, Gu and Jagtiani, 2020). FinTech has also furtherly digitized payment by the creation of e-wallets (Allen, Gu and Jagtiani, 2020), which through co-operations of card processors, non-bank, and bank entities allow users to have electronic wallets (Puschmann, 2016), functionally similar to both current accounts and standard debit cards. These systems are considered to be more inclusive, since some of their users might otherwise not have had access to traditional banking services (Allen, Gu and Jagtiani, 2020). Digital ledger technologies such as blockchains (and hence cryptocurrencies) also fall in this category (Goldstein, Jiang and Karolyi, 2019).

b) ***Advisory services:*** This is a broad category that refers to the implementation of FinTech within investment advice, asset and wealth management, insurance, and financial advice (Leong and Sung, 2018, Mehrban et al., 2020). FinTech services employ big data, machine and online learning and artificial intelligence to offer financial and wealth management and/or financial advice through the usage of large volume data pools (Gai, Qiu and Sun, 2017). FinTech also provides clear risk and capital management utilities (Wójcik, 2021), for example, the use of automated robo-advisors to ensure that a given portfolio is within a given risk tolerance, or that its attached risk does not exceed customers' preferences, being able to screen, implement and rebalance investment strategies on the go (Allen, Gu and Jagtiani, 2018). It also provides cheap, transparent, and open-access trading systems (Philippon, 2016). These same machine learning/AI techniques have also been applied to the insurance industry for client advice, risk management and evaluation and claims management (Puschamn, 2017). FinTech has also allowed for high-frequency trade through high-speed links, specialist algorithms and individual data feeds, including robo-investment (Allen, Gu and Jagtiani, 2020), allowing immediate trade and valuation of multiple assets globally.

c) ***Financing:*** FinTech provides new avenues of financing for both business and individuals, employing solutions focused on improving personalization, cost,

information sharing, flexibility, and effectiveness (Leong and Sung, 2018). Crowdfunding (including P2P lending) is one of such new avenues. Raising worldwide $305bn of capital in FY 2018 (Wójcik, 2021), it has become the most popular type of alternative finance due to its lower cost and early availability for start-ups (Leong and Sung, 2018). FinTech also enables the application of machine learning and artificial intelligence techniques to overcome the traditional limitations of credit scoring/credit risk on potential borrowers, particularly for those with thin credit files or unbanked (Allen, Gu and Jagtiani, 2018), while also processing lending applications much faster and without demand bottlenecks (Goldstein, Jiand and Karolyi, 2019).

1.2 New capabilities beget new vulnerabilities

For all the benefits FinTech brings to the financial sector, such a widespread and deep change in practices and procedures is not exempt of problems. Indeed, the sweeping changes brought by this comprehensive and ongoing industry-wide technological transformation have created new challenges for regulators and enforcers alike (Philippon, 2016), a reality which is being discussed by several authors (see among others Gai, Qiu and Sun, 2018, Lin and Chen, 2019, Mehrban et al., 2020, Allen, Gu and Jagtiani, 2020). For the purposes of this report some of the most outstanding issues discussed by scholars in the existing literature have been compiled in this section to provide a succinct overview of these concerns:

a) ***Privacy and data protection:*** This is considered to be the most significant (and complex) issue associated with the widespread implementation of FinTech (Mehrban et al., 2020), and is closely related to the critical task of private data carrying and subsequent storage (Gai, Qui and Sun, 2018). Many of the advantages offered by FinTech require data in exchange for a service or product (Dorfleitner, Hornuf and Kreppmeier, 2021). Consequently, problems related to privacy and data protection raise new questions in regards of ethical usage of data, both aggregate and raw, and of who should have control over these data to safeguard consumer privacy while avoiding systemic misuse (Allen, Gu and Jagtiani, 2020). Examples of this problematic areas are the vast data available on borrowers (Goldstein, Jian and Karolyi, 2019) or the use of personal alternative data in machine learning/AI processing of digital lending applications (Chou, 2020). These issues are fundamental precisely because privacy and data protection risks are linked to the business operations, outsourcing and financial data required by FinTech (Gai, Qui and Sun, 2018), and thus arise from the general use

of the technologies that these services are built upon (Allen, Gu and Jagtiani, 2020). Moreover, these risks may potentially happen during any part of the data usage cycle, including data storage and processing (Mehrban et al., 2020). As such, most research highlights major concerns on the privacy risks of using FinTech (Mehrban et al., 2020). Perhaps unsurprisingly, perceived private data security is a key determinant of users' FinTech adoption (Dorfleitner, Hornuf and Kreppmeier, 2021).

b) ***Cybersecurity:*** A second, but arguably equally important concern discussed in the existing research is that of cybersecurity, with new services necessarily breeding new risks (Mehrban et al., 2020, Miyauchi, 2021). As an example, it is worth noting that the financial industry has suffered the most incidents involving data loss because of a cyber-attack (Allen, Gu and Jagtiani, 2020. This fact must be combined with the relevance of Start-ups in the FinTech environment, which are companies who usually do not have comprehensive cybersecurity to begin with (Worthalter, 2021, Kaur et al., 2021a). Furthermore, cyber risks have become increasingly complex as the service models have enlarged, and are generally classified by their scope into operational, tactical and strategical cyber risks (Mehrban et al., 2020, Kareem et al., 2020, Miyauchi, 2021). Again, as with privacy risks, the potential for a security breach in cloud networks causing the loss of vast financial data is a risk in-built in the technologies used to operate FinTech themselves (Goldstein, 2019, Smith, 2020b). Cyber-attacks targeting FinTech providers can be generally classified either as unauthorized accesses, illegal money transfers, targeted attacks, and Denial of Service (DoS/DDoS) attacks (Miyauchi, 2021, Kaur et al., 2021b). Because of these intrinsic vulnerabilities, FinTech providers must spend more resources than physical providers on cybersecurity measures (Chou, 2020), and need to upscale their budget allocations for hardware, software, and personnel (Worthalter, 2021). This has in turn created a FinTech-specific professional market focused on cybersecurity advisory services, involving policies, training, IT, technical and cyber-insurance services (Smith, 2020a, Smith 2020b). Further evidence of this drive towards a more comprehensive approach for cybersecurity, perceived as an endemic issue of FinTech can be seen in the increasing number of public-private partnerships pursuant to increase industry resilience and risk mitigation (Kwok, 2017).

c) ***Fraud:*** The third widespread vulnerability identified in the literature is fraud. While fraud is certainly not a new phenomenon, the quick expansion of FinTech has either created new patterns of commission or altered existing fraudulent practices. Examples of this include fraudulent transactions from digital wallets (Kaur et al, 2021b),

fraudulent approval of borrowers in P2P lending (Gallo, 2021) or credit card fraud associated to data theft from insecure servers (Kaur et al., 2021a). Addressing fraud risk is therefore fundamental for FinTech business (Allen, Gu and Jagtiani, 2020). While fraud in FinTech is largely similar to that occurring in other sectors, being driven by common general factors such as pressure to meet targets and untried business models with enhanced exposure to fraud (Kwok, 2017), FinTech fraud generally employs more technologically sophisticated means for the commission and concealment of the offenses (Kwok, 2017). As such, digital lenders require more resource-intensive measures for fraud detection and prevention than other financial actors in this ecosystem (Chou, 2020). Moreover, while FinTech has also meant easier access to financial services for customers who have not had access to them in the past, this less financially literate population is in turn much more vulnerable to fraud (Panos and Wilson, 2020). Considering this increasingly complex operative environment, big data resources paired with artificial intelligence and machine learning are being employed to craft advanced fraud detection systems (Allen, Gu and Jagtiani, 2020). These systems are unfortunately still far from perfect, and even sophisticated screening procedures for online lending services are still ineffective at detecting borrowers' misreporting (Gallo, 2021). While indeed FinTech-related financial fraud is proving to be greater societal risk than anticipated, ML/AI solutions are quickly improving in the realm of anomaly detection at a high enough pace to ensure that they will remain a cornerstone resource in the fraud prevention toolkit of financial institutions (Stojanovic et al., 2021).

2. Fintech and crime: Mapping the State of the Art

Academic and practitioner-led scholarship in FinTech is increasing at a rapid pace, particularly among young scholars (Goldstein, Jiang and Karolyi, 2019). While around five years ago there was a marked lack of general scholarship interested in scrutinizing FinTech (Leong and Sung, 2018), with comprehensive literature reviews yielding roughly 200 articles regarding FinTech spread across 10 databases (Schueffel, 2016), at the turn of the decade a single call for papers yielded updwards of 150 proposals from 200 organizations and 400 authors (Goldstein, Jiang and Karolyi, 2019). Given this expanding interest and considering the issues associated with the widespread rollout of Fintech across the financial sector such as security, data privacy, operational threats and cyber-attacks (Mehrban, 2020) discussed in the previous heading, there is a coalescing

body of academic work that is exploring the nexus between FinTech and crime broadly understood. From the literature reviewed for this report, it emerged that research into FinTech and its implications for crime (understanding as such offending, victimization, technological capabilities to commit and conceal offences, etc.), can generally be classified as belonging to one or several of the following nodes: (a) research into FinTech and financial/insurance fraud, (b) research into FinTech and cybersecurity/data privacy, (c) research into illicit uses of blockchains and FinTech and money laundering. These are almost a mirror-like match to the issues generally explored in the previous heading, and the state of the art of these fields will be summarily discussed in the following headings.

2.1. Fraud research

Within fraud research there are two distinct currents of inquiry, targeting two different phenomena: fraudulent transactions and fraudulent borrowing in P2P lending. The former is mostly descriptive, without using other data than case studies as examples, and aims to contextualize fraudulent transactions within FinTech as an evolving phenomenon (see for example Miyauchi, 2021). These are, in essence, variations on credit card/transfer frauds facilitated by FinTech due to the entirely cyber nature of the financial operations (Kaur et al., 2021a), but not new phenomena in themselves. In this sense, FinTech acts as a new technical ground upon which different fraud offences can be committed (Kaur et al., 2021b), but does not necessarily create or enables entirely new forms of fraud in itself. Research seems to point out that it is just a case of FinTech services being more vulnerable by design than traditional banking, insofar as they attract comparatively a high percentage of committed fraud (Omodero, 2021), but data on this regard remains limited. Consequently, a stream of literature has emerged which tackles technology-driven, data-rich proposals to enhance fraud prevention within these systems. Several AI-based techniques are explored in the literature, such as incremental learning, which shows promise as a GDPR compliant tool to adequately assess and prevent fraudulent operations while overcoming the technical complexities of preventing digital credit card fraud (Lebichot et al., 2021). Other forms of machine learning are also showing promising results. Synthetic data is being employed in the field of credit card and transaction frauds, to create pre-emptive solutions based on anomaly detection (Stojanovic et al., 2021). But these mechanisms of fraud detection and prevention have been problematized, insofar as they might potentially present privacy issues with the data they employ or with how intrusive they are for the user, and although existing research showcases that this is so far not being the case (Găbudeanu et al., 2021), such potentiality is acknowledged.

The second phenomena, fraud in P2P lending, is however an entirely new FinTech issue which did not exist in traditional financial services. This fraud refers to borrowers on online lending platforms misrepresenting their relevant financial details to obtain lent money that otherwise would have been denied by said platforms, and which will be later defaulted on. The literature showcases the difficult balance that these lenders navigate between minimizing potential fraud risk and maximizing loan volume for increased profit (Gallo, 2021, Li et al., 2021). Research trying to unravel the complex relation between borrower screening and data misrepresentation concludes that P2P lending platforms are still unable to detect some types of fraudulent borrowers (Gallo, 2021). Indeed, some researchers are positing that this enhanced fraud risk is part and parcel of P2P lending platforms, with in-depth case studies from China, once world-leading in P2P lending, being cautionary tales about the limitations of a technology-based approach to risk mitigation and fraud detection resting upon insufficient regulatory frameworks (Chen et al., 2021). In spite of this, there is still literature exploring the possibilities of purely technological solutions for borrower screening, and also, interestingly, for early defaulting as well, emphasizing the problem inherent to fraud detection of extremely imbalanced samples, while positing ways in which these can be overcome with algorithmic approaches including cost-benefit balances (Li et al., 2021). But again, the application of these ML/AI technologies for borrower screening and loan fraud prevention raises key ethical questions that are only beginning to be explored in this context now, such as race and gender bias, which evidence shows are unduly affecting algorithmic procedures (Bertoni et al., 2021)

2.2. Cybersecurity research

The second general research cluster is focused on the cybersecurity concerns in the FinTech ecosystem. Research showcases that the mere penetration of newer technologies in the financial sector has meant inexorably an increase in cybersecurity risks of various kinds (Najaf, Mostafiz and Najaz, 2021, with an exhaustive list of threats also provided in Kaur et al., 2021b). Having explored in the first section of this report some of those overarching cybersecurity issues pertaining FinTech itself, further research highlights the fact that cybersecurity risks evolve as quickly as the services offered by FinTech itself (Uddin, Mollah and Ali, 2020). Unsurprisingly, victimization of both individuals and corporations by cybersecurity breaches is increasing over time (Chung et al., 2021). Research showcases that in the implementation of cybersecurity measures in FinTech and other cyber-complex systems, the weakest link in the chain remains the end user, which should be the focus for future protective/pre-emptive programs (Chung et al., 2021). This end-user focus is particularly relevant in the FinTech customer base, which as we have discussed in the previous heading, can be less financially literate than the customers of traditional financial providers (Panos and Wilson, 2020). Recently, prospective literature

reviews signalled that despite the huge maintenance and implementation costs involving the adoption of AI systems for cybersecurity, anomaly detection, deep learning, machine learning, and predictive analytics, these measures are being embraced as necessary cybersecurity tools within the industry (Gandhour, 2021).

There seems to be agreement that going forward we can expect an increase in testing, development and refining related activities within the specific sector of cybersecurity applications of IA, which will be fundamental for the FinTech industry (Smith, 2020, Gandhour, 2021). Nevertheless, it must be underscored that the expectations of both clients and practitioners in regards of what these technologies can offer must be rationalized (Smith, 2021). In sum, research seems to point out that in FinTech cybersecurity is so relevant that it must evolve from a purely technical concern and become an organizational concern (Smith, 2021). Existing research, however, does not elaborate on the specifics of how that holistic approach might be best achieved. Nevertheless, it is acknowledged that such perspective is the gold standard, and that adequate risk response always ought to be operationalized not only through technical axes, but also through organizational and human countermeasures, which must be kept fluid as the risks evolve (Miyauchi, 2021). These comprehensive approaches match closely the FinTech specific vulnerabilities identified by Kaur et al. (2021a), which included technological concerns aside from human and operative ones, that need to be paired with adequate threat intelligence and structured threat modelling (Kaur et al., 2021b).

2.3. Blockchain research

The third general research cluster in the current FinTech literature is focused around blockchain and its applications. Blockchain, a distributed ledger technology (DLT), came into relevance for the FinTech sector in 2008 when its application materialized into Bitcoin in 2008 (Wojcik, 2021). These DLT-based tokens became then known as cryptocurrencies. However, blockchain in itself is an infrastructural technology, and thus its usefulness is not limited to just cryptocurrencies, being possible to leverage it as well into cybersecurity applications (Parizi et al., 2021). Blockchains can be private, permissioned, or public, depending on the distributing of writing privileges (Allen, Gu and Jagtiani, 2020). Significantly, blockchain was discussed in a very substantial part of the literature reviewed, with references or mentions appearing on upwards of a 30% of the material, even though in practice, as the review of Dorfleitner et al. (2021) illustrates, blockchain and cryptocurrencies represent less than a 1% of FinTech companies in their sample. This dissonance between actual business impact and academic scrutiny may be due to the fact that it has been considered as a “next-generation” technology for already more than 15 years (Chen et al., 2021), becoming very much a buzzword (Allen, Gu and Jagtiani, 2020). Nowadays, even scholars that define blockchain as a potential paradigm-shifting

technology capable of revolutionizing the financial services industry caution that it is but a technological tool in the end (Smith, 2020b).

As any new technology, however, it presents a variety of issues directly related to crime and its peripheral research disciplines. For one, its entirely decentralized nature presents huge regulatory and enforcement challenges, riddled with parochial nuance (Bertoni et al., 2021). Blockchains have a complex functioning in which blocks of records containing a cryptographic hash of the previous block, a timestamp, and transactional data linked together are designed precisely to be secure, resistant to external modification and tamper-proof (Allen, Gu and Jagtiani, 2021, Stojanovic et al., 2021). As such, there is a wealth of cutting-edge cybersecurity applications based on different blockchains (Parizi, et al., 2020). However, in reality blockchain hast not been as resilient as expected, with cases such as Goldfinger attacks, feather-forking or 51% attacks, specific cybercriminal techniques employed for fraudulent exploitation (Miyauchi, 2021, Stojanovic et al., 2021). Unsurprisingly given this complexity, many organizations, even within the FinTech sector, do not have the internal expertise to create in-house blockchain applications (Smith, 2020b). But externalization may not be an option either: the lack of general training and development of would-be operators not only impeding the employment of blockchain-based applications, but also risking an increase in inefficiency and errors (Smith, 2020b).

The literature has also identified cyber-risks not intrinsically related to the technology itself, such as the existence of Ponzi schemes applied to different frauds related to blockchain-based currencies (Stojanovic et al., 2021). But the important takeaway is that the in-principle secure design for which blockchains are known does not mean that there are no cybersecurity concerns. In fact, due to its technical complexity and the lack of institutional and corporate knowledge with blockchain as a resource, the risks of its application can be often understated (Smith, 2020a).

2.4. Money laundering research

The last research cluster or topic identified in regards of criminal activities in the FinTech ecosystem pertains money laundering. The field of money laundering within FinTech is generally approached in two distinct ways. The first identifies FinTech as a set of technologies which create new risks in regards of money laundering, but just as most financial institutions do through regular non-compliance (Kaur et al., 2021). In this sense, risk is enhanced because FinTech allows an increasing volume of transactions (Faccia, 202) to happen in very small amounts of time, over interactive networks operative at all times, and can easily encompass problematic areas including de-regulated free trade zones (Stojanovic et al., 2021). Within this field of inquiry, relevance is given to the role of cryptocurrencies as a tool used for money laundering (Allen, Gu and Jagtiani, 2020): new cryptocurrencies allow for

payments to be made in completely new ways, which allow both extreme privacy (Kareem et al., 2020) and a good degree of anonymity (Faccia, 2020), while the growing theft of cryptocurrencies simultaneously making anti-money laundering operations more complex and technical (Allen, Gu and Jagtiani, 2020).

The inherent characteristics of cryptocurrencies allow for complex laundering processes to be emplaced, usually involving *layering* (purchase of cryptocurrencies with the money to be laundered, then using mixers and tumblers to move it around with great anonymity and difficult traceability) and *integration*, in which the diversified cryptocurrencies are then re-exchanged for FIAT currencies through connected bank accounts or used for real state purchases (Allen, Gu and Jagtiani, 2020, Faccia, 2020). This off-ramp, in which cryptocurrencies are reverted to FIAT currency, is the most well-guarded part of the process from an enforcement perspective (Dupuis and Gleason, 2021). Case analysis demonstrates that these methods have been successfully employed, with individuals laundering upwards of 350 million euros through major trading platforms and cryptocurrency exchanges. Another laundering opportunity arises in virtual markets that allow the cheap sale of FIAT currency of illicit origin in exchange for legitimate cryptocurrency, with laundering commissions reaching up to 90% (Faccia et al., 2020). However, these money laundering operations still have limitations, requiring either the usage of tumbling services (mixers) or complex simultaneous operations on over-the-counter markets (Dupuis and Gleason, 2021). FinTech has however not only created new ways of money laundering, like the use of cryptocurrency mixers or cryptocurrency wallets/portfolios, it has also allowed traditional money launderers to upscale their operations, with Danske Bank and Deutsche Bank laundering up to 200 billion euros in a seven-year period (Faccia et al., 2020) a feat that required the speed and diversity of transactions that only FinTech can deliver.

The other way in which the relation between FinTech and money laundering is scrutinized is that of pre-emptive or disruptive applications. As the report discussed in its opening, FinTech is just a series of varied and complex technologies, and therefore, these can also be deployed proactively to combat money laundering. Some of the ways in which this can be done involve network analysis with automated data mining, in which machine learning uses real cases of money laundering, or algorithmic detection of suspicious activities (Stojanovic et al, 2021). These are potent analytical tools with the ability to use real time transactional data or synthetic data for benchmarks and demonstrate that machine learning can support enhanced detection capability, allowing for extreme finetuning (Stojanovic et al, 2021). Reports illustrate that there are nascent research communities concerned with furthering the applications of specific forms of data mining and machine learning for anti-money laundering FinTech, using increasingly complex and interdependent techniques (Pang et al., 2021). This allows to complement human-led anti-money laundering initiatives within relevant stakeholders,

escalating their capability through automated and evolving anomaly detection supporting these teams (Faccia, 2020). The technical push is moreover accompanied by an academic drive that acknowledges the need for further regulation within FinTech. Particularly, in payment services and cryptocurrencies, it is considered a prerequisite step for any successful countering of money laundering (Nikiforova and Nikiforov, 2021). This is however not unproblematic given the inherent difficulties of regulating such a decentralized and trans-national phenomenon (see among others Philippon, 2016 and Bertoni et al., 2021). Moreover, researchers posit that while a regulatory drive could aspire to tackle current techniques of money laundering through FinTech and particularly cryptocurrencies, new techniques and methods will emerge to bypass these barriers (Dupuis and Gleason, 2021).

3. Data sources

Having mapped in the previous heading the published research pertaining the aspects of FinTech that are of interest to the study of crime and its adjacent disciplines, this report will now focus on providing an overview of the data sources that are being used in these efforts, while discussing their possible future use, and their relative strengths and shortcomings. To do so, distinction will be made between synthetic data and real-world data.

3.1 Synthetic data

Synthetic data has not been extensively used in the reviewed research, but this does not mean that there are not cases in which it is employed, and that it cannot be a most useful tool in researching Fintech from a crime-sensitive perspective. Synthetic data has been used specifically within risk management/fraud detection in FinTech, particularly for the deployment and testing of algorithmic tools (Chen, Yu and Dargahi, 2021, Stojanovic et al., 2021)[1]. Synthetic datasets based upon simulations of proprietary datasets (such as aggregated financial transactional data or aggregated mobile payment data) allow researchers to explore machine learning and AI security solutions without the need to access extremely sensitive and, from a privacy perspective, ethically problematic data (see among others Stojanovic et al., 2021). These synthetic datasets are accessed usually via the Kaggle on-line data science community, which indexes both synthetic and real-world open databases. So far,

[1] Some of the relevant synthetic datasets are the following:
https://www.kaggle.com/ealaxi/paysim1
https://www.kaggle.com/ealaxi/banksim1

however, it is worth noting that synthetic data has seen limited use in FinTech related research, and only pertaining to machine learning related algorithms.

3.2 Real-world data

By contrast with synthetic data, many different types of real-world data are employed in FinTech-related research, both within quantitative and qualitative perspectives. While it is impossible to discuss all the plausible data sources, or indeed, all the data sources used in the current FinTech literature, some of the most prominent ones will be tackled now. As with synthetic data, Kaggle also provides open access real-world datasets of high relevance, such as credit card fraud detection data (Stojanovic et al., 2021)[2]. Besides open access datasets, when it comes to real data, proprietary datasets are also employed. These are usually accessed through research partnerships or commercial collaborations, are quite rare, and can be seen frequently upcycled on posterior works by other scholars (for an example of first-hand use of proprietary real-world data in FinTech see Juszczak et al., 2008). Besides aggregated datasets, FinTech research also relies heavily on case studies. Examples of these can be found among others in Faccia et al. (2020). It must be understood however that in said review all case data came from open sources which had to be both available and verifiable, which can generally limit the amount of overall data that can be the basis for case analysis.

Lastly, another source of real-world data that is widely employed in FinTech research is grey literature. Data contained in reports (such as Capgemini's annual World FinTech Report), briefs (such as CrowfundingHub research briefs) and executive summaries (sometimes available by FinTech service providers) provide valuable and useful data for research into FinTech and its implications for various forms of crime, victimisation, policy responses, cybersecurity, and many other related fields of inquiry. It is worth noting, however, that FinTech research appears so far characterized by a marked reliance on secondary data entirely, with no purpose-built data collection being employed so far in any of the recent literature. While certainly it is complex to obtain primary data in this field, research so far seems to be limited to entirely opportunistic data access.

[2] Some of these open datasets can be accessed by the following links:
https://www.kaggle.com/mlg-ulb/creditcardfraud
https://www.kaggle.com/apoorvwatsky/bank-transaction-data
https://www.kaggle.com/bigquery/bitcoin-blockchain

4. The COVID-19 context in the FinTech ecosystem

In spite of the fact that most of the reviewed works were published either during or after the first stages of the COVID-19 pandemic, its influence does not play a central role in the current FinTech literature, and in fact, it is seldomly discussed. There are nevertheless some works focused on its impact (see Fu and Mishra, 2020, or Kehinde and Eskin, 2020, among others), and these ripple through a fraction of the literature, although this practice remains minoritarian. Among the authors that do factor in COVID in their research, there seems to be an agreement on the fact that the pandemic has reshaped all economic activity in general (Gallo, 2021, Bertoni et al., 2021). And while this impact has been highly heterogeneous, it has meant a decline in access to traditional financial services (Bertoni, 2021). As such it has highlighted the value of the more efficient FinTech solutions spread across the full financial ecosystem (Faccia et al., 2020). In short, it is argued that the COVID-19 context has contributed to expedite a shift towards digitized financial services, and particularly, attracted customers towards FinTech-mediated forms of lending (Allen, Gu and Jagtiani, 2020) such as P2P loans and AI/ML approved lending.

Besides this increment in risk associated to an increment in operations, COVID-19 specific risks have also been identified in the literature. Given the reliance of FinTech in digital platforms, there have been identified vulnerabilities relating to phishing attacks and online banking trojans which used COVID-19 information and COVID-19 specific means of contact, such as emails or instantaneous messages (Kaur et al., 2021). Noteworthy in the FinTech realm, and entirely contemporary to the pandemic, is the non-fungible tokens (NFTs) craze. NFTs are digital assets authenticated through a public blockchain, and they have seen a veritable boom (Mackenzie and Bērziņa, 2021 and Jordanoska, 2021). These are a form of digital collectibles that can represent either digital art or other digital goods, and as such, they can and are subjected to the same forms of criminality that those goods in their traditional, physical, form can, such as theft, stolen goods handling and fraud (Mackenzie and Bērziņa, 2021 and Jordanoska, 2021). And these implications are extremely serious with NFTs being sold for hundreds of thousands of dollars. A single documented scam costing a collector £244,000 worth of Ethereum cryptocurrency (Jordanoska, 2021). Currently NFT trading offers extremely high profit margins in a hyped marked with manufactured scarcity (Mackenzie and Bērziņa, 2021). This, combined with its good degree of anonymity, de-regulated offer-and-demand value and quick trading, makes NFTs an ideal tool for fraud and money laundering (Jordanoska, 2021). Research on this field is, however, only sprouting now.

5. Charting the way forward: research gaps

From the current state of the art several research gaps can be identified that ought to be tackled in the future, and which can substantially contribute to the field. When discussing prospective research, however, it is important to note the fact that the COVID-19 pandemic is not yet over. Combining this with the pace of academic publishing, which can be sometimes not-so-brisk, it can be expected that more studies regarding this particular context will appear in the near future. Arguably it can be presumed that these will pertain both its long- and short-term impact within the FinTech ecosystem and its relationship with risk and crime specifically. That said, an avenue of inquiry that must be further explored is *the understanding of user confidence in the security and privacy of FinTech from both an end-user (customer) perspective and operational user (business) perspective*, with a focus on what makes them perceive these cluster of technologies as secure or insecure, and how do they navigate their associated security and privacy issues. This has already been problematized by some researchers (Mehrban et al, 2020), and it appears fundamental to understand risk management and technology adoption.

While to date the two areas of FinTech that have attracted most research are generally speaking crowdfunding (including peer-to-peer lending) and blockchain (including cryptocurrencies) (Cai, 2018; Xu et al., 2019), this does not mean that these fields are exhausted. As discussed in the previous heading, further research is necessary in regards of blockchain to better understand the NFT phenomena, and its potential risks and vulnerabilities *vis-à-vis* criminal activities and how to address them. This is not only topical, but also urgent, as the NFT markets rapidly expand. Other peripheral areas also need further development and attention. While there is a growing literature on how FinTech, through cryptocurrencies, can enable and facilitate new forms of money laundering, very little heed is paid at how FinTech enables traditional financial actors such as banks to launder money in more efficient and safe ways, despite the public case evidence of these practices discussed elsewhere in this report, and the huge volumes of assets they entail.

Ultimately, it would also be desirable to start imbricating primary data across the different research fields pertaining FinTech. Although some of the difficulties of doing so have been summarily discussed in the Data Sources heading, it represents an opportunity to further enrich FinTech research, particularly at the crossroads of FinTech and Crime, the benefits of using secondary (and even synthetic) data notwithstanding.

6. Bibliography

Allen, F., Gu, X., & Jagtiani, J. (2020). A Survey of Fintech Research and Policy Discussion. *Review of Corporate Finance*, *1*(3–4), 259–339. https://doi.org/10.21799/frbp.wp.2020.21

Benny, K. (2017). Emergence of Fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation & Compliance*, *25*(4), 422–434.

Bertoni, F., Bonini, S., Capizzi, V., Colombo, M. G., & Manigart, S. (2021). Digitization in the Market for Entrepreneurial Finance: Innovative Business Models and New Financing Channels. *Entrepreneurship: Theory and Practice*, 1–16. https://doi.org/10.1177/10422587211038480

Chen, D., Deakin, S., Johnston, A., & Wang, B. (2021). Too Much Technology and Too Little Regulation? The Spectacular Demise of P2P Lending in China. *Accounting, Economics and Law: A Convivium*. https://doi.org/10.1515/ael-2021-0056

Chou, A. (2020). WHAT ' S IN THE " BLACK BOX "? BALANCING FINANCIAL INCLUSION AND PRIVACY IN. *Duke Law Journal*, *69*(5), 1183–1218.

Chen, K.-C., Yu, C.-M., & Dargahi, T. (2021). Evaluating the risk of disclosure and utility in a synthetic dataset. *Computers, Materials & Continua*.

Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2021). Promise Not Fulfilled: Fintech Data Privacy, and the GDPR. *SSRN Electronic Journal*, *October*. https://doi.org/10.2139/ssrn.3950094

Dupuis, D., & Gleason, K. (2021). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, *28*(1), 60–74. https://doi.org/10.1108/JFC-06-2020-0113

Faccia, A., Moçteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020). Electronic Money Laundering, the Dark Side of Fintech: An Overview of the Most Recent Cases. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*, 29–34. https://doi.org/10.1145/3430279.3430284

Fu, J., & Mishra, M. (2021). Fintech in the time of COVID-19: Technological adoption during crises. *Journal of Financial Intermediation*, 100945.

Gabudeanu, L., Brici, I., Mare, C., Mihai, I. C., & Scheau, M. C. (2021). Privacy intrusiveness in financial-banking fraud detection. *Risks*, *9*(6). https://doi.org/10.3390/risks9060104

Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications*, *103*, 262–273.

Gallo, S. (2021). Fintech platforms: Lax or careful borrowers' screening? *Financial Innovation*, *7*(1). https://doi.org/10.1186/s40854-021-00272-y

Goldstein, I., Jiang, W., & Karolyi, G. A. (2019). To FinTech and beyond. *Review of Financial Studies*, *32*(5), 1647–1661. https://doi.org/10.1093/rfs/hhz025

Jordanoska, A. (2021). The exciting world of NFTs: a consideration of regulatory and financial crime risks. *BUTTERWORTHS JOURNAL OF INTERNATIONAL BANKING AND FINANCIAL LAW*, 10, 716.

Kareem, H. M., Duhaidahawi, A., Zhang, J., & Abdulreza, M. S. (2020). Analysing the effects of FinTech variables on cybersecurity : Evidence form Iraqi Banks. *International Journal of Research in Business and Social Science*, *9*(6), 123–133.

Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). *Cybersecurity Vulnerabilities in FinTech*. 89–102. https://doi.org/10.1007/978-3-030-79915-1_5

Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). *Cybersecurity Threats in FinTech*. 65–87. https://doi.org/10.1007/978-3-030-79915-1_4

Kehinde T and Eksin T (2020) How fintech can help SMES recover from the impact of COVID-19. Available at: https://www.weforum.org/agenda/2020/05/fintech- can-help-smes-recover-covid-19/ (accessed

Lebichot, B., Paldino, G. M., Siblini, W., He-Guelton, L., Oblé, F., & Bontempi, G. (2021). Incremental learning strategies for credit cards fraud detection. *International Journal of Data Science and Analytics*, *12*(2), 165–174. https://doi.org/10.1007/s41060-021-00258-0

Leong, K. (2018). FinTech (Financial Technology): What is It and How to Use Technologies to Create Business Value in Fintech Way? *International Journal of Innovation, Management and Technology*, *9*(2), 74–78. https://doi.org/10.18178/ijimt.2018.9.2.791

Li, Z., Zhang, J., Yao, X., & Kou, G. (2021). How to identify early defaults in online lending: A cost-sensitive multi-layer learning framework. *Knowledge-Based Systems*, *221*, 106963. https://doi.org/10.1016/j.knosys.2021.106963

Mackenzie, S., & Bērziņa, D. (2021). NFTs: Digital things and their criminal lives. *Crime, Media, Culture*, 17416590211039797

Mehrban, S., Khan, M. A., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., Kiah, M. L. M., Abbas, F., & Hassan, M. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *IEEE Access*, *8*, 23391–23406. https://doi.org/10.1109/ACCESS.2020.2970430

Miyauchi, Y. (2021). The Economics of Fintech. In *The Economics of Fintech* (Issue 1). Springer Singapore. https://doi.org/10.1007/978-981-33-4913-1

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*, 2150019.

Nikiforova, V. D., & Nikiforov, A. A. (2021). State Regulation of Blockchain Technology in the Sphere of Payments and Financial Services. In *Studies in Systems, Decision and Control* (Vol. 314). Springer International Publishing. https://doi.org/10.1007/978-3-030-56433-9_9

Omodero, C. O. (2021). Fintech Innovation in the Financial Sector: Influence of E-Money Products on a Growing Economy. *Studia Universitatis „Vasile Goldis" Arad – Economics Series*, *31*(4), 40–53. https://doi.org/10.2478/sues-2021-0018

Pang, G., Li, J., Van Den Hengel, A., Cao, L., & Dietterich, T. G. (2021). Anomaly and Novelty Detection, Explanation, and Accommodation (ANDEA). *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 4145–4146. https://doi.org/10.1145/3447548.3469453

Panos, G. A., & Wilson, J. O. S. (2020). Financial literacy and responsible finance in the FinTech era: capabilities and challenges. *European Journal of Finance*, *26*(4–5), 297–301. https://doi.org/10.1080/1351847X.2020.1717569

Parizi, R. M., Dehghantanha, A., Azmoodeh, A., & Choo, K. K. R. (2020). Blockchain in cybersecurity realm: An overview. *Advances in Information Security*, *79*, 1–5. https://doi.org/10.1007/978-3-030-38181-3_1

Philippon, T. (2016). *The fintech opportunity*. National Bureau of Economic Research.

Puschmann, T. (2017). Fintech. *Business and Information Systems Engineering*, *59*(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

Schueffel, P. (2016). Taming the beast: A scientific definition of fintech. *Journal of Innovation Management*, *4*(4), 32–54. https://doi.org/10.24840/2183-0606_004.004_0004

Smith, S. S. (2020). Cybersecurity & Insurance. In *Blockchain, Artificial Intelligence and Financial Services* (pp. 193–200).

Smith, S. S. (2020). Emerging Technologies and Implications for Financial Cybersecurity. *International Journal of Economics and Financial Issues*, *10*(1), 27–32. https://doi.org/10.32479/ijefi.8844

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in fintech applications. *Sensors*, *21*(5), 1–43. https://doi.org/10.3390/s21051594

Wójcik, D. (2021). Financial Geography I: Exploring FinTech – Maps and concepts. *Progress in Human Geography*, *45*(3), 566–576. https://doi.org/10.1177/0309132520952865

Worthalter, E. (2021). Fintech's need for holistic security. *Computer Fraud & Security*, *2021*(12), 10–13. https://doi.org/10.1016/S1361-3723(21)00128-7