CRYPTOGRAPHY IN FINANCIAL MARKETS: POTENTIAL CHANNELS FOR FUTURE FINANCIAL STABILITY

Alim Al Ayub Ahmed, Jiujiang University, China
Harish Paruchuri, Anthem, Inc., USA
Siddhartha Vadlamudi, Xandr, USA
Apoorva Ganapathy, Adobe Systems, USA

ABSTRACT

Digital finance is assuming a significant part in the arrangement of financial services all over the world. Fast growth with digitalization, data analysis, and computing capacities allows for a whole new scope of financial services and transactions. This financial development empowered by digital financial technology (Fintech) has pulled in a ton of attention, as it could offer some potential for economic growth and development. As a part of the Fintech environment, cryptography has started to grow quickly and digital assets are acquiring in favorability among financial bankers and investors. Human behavior as they engage with financial activities is personally associated with the noticed market elements. However, with many existing theories and studies on the fundamental motivations of the conduct of people in financial frameworks, there is still restricted experimental derivation of the behavioral conduct of the financial agents from a definite market analysis. Cryptocurrency technology has given a map to this analysis with its voluminous data and its transparency of financial transactions. It has empowered us to perform inference on the personal conduct standards of users in the market, which we analyze in the bitcoin and ethereum cryptocurrency markets. In our study, we initially decide different properties of the cryptography users by complex network analysis. Financial cryptography is a difficult subject that necessitates abilities from a variety of seemingly unrelated fields. There is a serious risk that attempts to establish Financial Cryptography frameworks would simplify or omit key disciplines because they are caught between central banking and cryptography. This paper discusses research that attempts to limit the scope of Financial Cryptography. This model should assist the project, administrative, and requirements personnel by classifying each discipline into a seven-layer model of basic nature, where the link between each adjoining layer is evident. While this model is shown as effective, all models have cutoff points. This one does not present a design system or a protocol agenda. Furthermore, given the model's initial adaptation and the field, it should be viewed as a suggestion of complexity rather than a definitive approach.

Keywords: Cryptography, Financial Markets, Cryptocurrency, Financial Stability.

INTRODUCTION

Cryptocurrencies keep on drawing a lot of attention from investors, business visionaries, regulators, and the overall population. Various new open discussions of cryptocurrencies have been started by the considerable changes in their costs, ensures that the market for cryptocurrencies is an air pocket with no basic worth. These concerns have prompted calls for expanded regulation or even an absolute boycott. Further discussions concern: the arrangement of cryptocurrencies as

commodities, cash, or something different; the expected development of cryptocurrency derivatives and credit contracts in cryptocurrency; the usage of initial coin offerings pursuing cryptocurrency to finance start-ups; and the issue of digital currencies by national banks using cryptocurrency. These discussions regularly shed more heat than light. There is very little established logical information about the markets for cryptocurrencies and their effect on economies, organizations, and individuals – now and in the future.

Cryptocurrencies are digital financial assets, for which records and transfers of proprietorship are ensured by crypto- graphic technology instead of a bank or other confided in the third party (Ahmed, 2020). They can be considered as financial assets because they bear some incentive for cryptocurrency holders, even though they represent no liability obligation of some other party and are not supported by any actual asset of significant worth (like gold, for instance, or stock of a company). While most cryptographic work for exchanges aims to conceal data, our goal is to enable a market designer to combine an appropriate amount of fractional simplicity with the provably correct behavior. We also do it in a scenario that is informed by real-world demands, such as trade with both limit and market disciplines, and where multi-party calculation by all parties is impossible (Vadlamudi et al., 2021). Our research looks at how to market designers specify exactly what they want to expose and only release that data while showing it, ensuring that market behavior is correct. This study has already been put to good use in avoiding unethical and parasitic trade activities in major deals, as well as giving a technique for exchanging massive block orders without revealing data that can be misused.

Issues will definitely arise at a particularly difficult point with so many knowledge bases. Not only is there inexorable confusion and wasted resources, but it's also difficult to find technical management and marketing talent who can only work in the field. It is a better practice to structure these disciplines into models that govern discourse, correlations, and decision making as key progress toward a better understanding of financial cryptography (Maleque et al., 2010). As an introduction to more noteworthy learning, this paper describes one such model that aims to portray the field in a straightforward manner. The names finance and cryptography is stretched out in this approach to highlight the disciplines that may have been hidden underneath the label. Obviously, no model can possibly cover the breadth and complexity of such a complex topic. The purpose of this present approach is to allow the reader to envision the entire field while also identifying the links between various disciplines without having to expend additional work and time on the specifics of each section. In this scenario, depth is sacrificed in favor of breadth.

INTRODUCTION TO FINANCIAL MARKETS

In this section, we'll go through how shares are traded to help people who don't have a background in finance get started. Our paper is best served by a study of market microstructure in finance. We found three market microstructure research publications (Biais et al., 2005; Madhavan, 2000; Stoll, 2003; Paruchuri, 2020) that helped us outline the foundation of our study. We simplify the complicated actions of current financial markets in many cases in order to explain the rules that apply to our job. In this study, we clearly establish these simplifying assumptions.

There is no substantial difference between dealers, brokers, financial specialists, or investors when it comes to the reasoning behind the cryptographic features of our study. In an ideal approach, everyone has access to the same data and can place limited orders. As a result, there are roughly two kinds of members: (market) operators, such as the exchange or its agent, and dealers, which include financial professionals, intermediary/sellers, institutional and retail investors, and so on (Zhu et al., 2021). In current financial markets, orders fall into two essential classifications:

market orders are an instruction to purchase or sell a particular amount of security and are filled when possible at the best available cost on the market, and limit orders are an instruction to purchase or sell a particular amount of a security at a particular cost and are filled just when another member in the market will make the opposite trade (Paruchuri et al., 2021) in Figure 1.

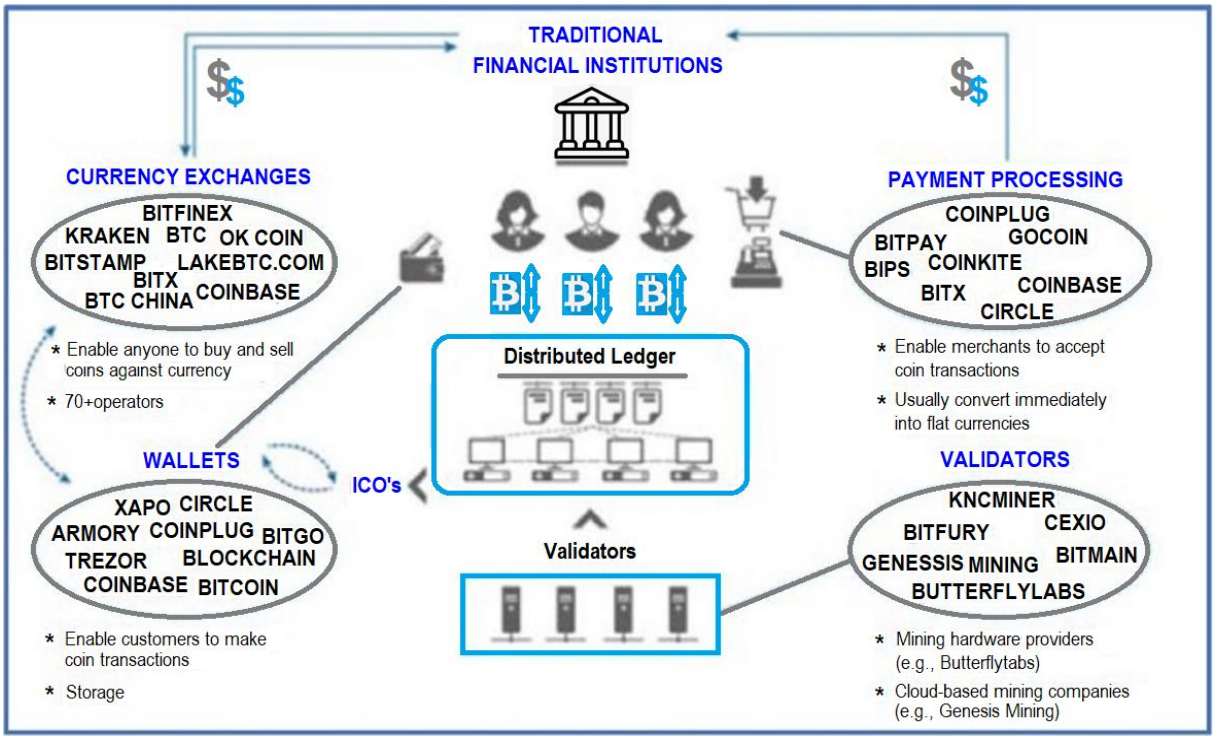

Figure 1
OPERATIONAL MODEL OF CRYPTOGRAPHY IN FINANCIAL MARKETS

Financial Market Information and Its Misuse

In this section, we'll look at how transparency can be used, as well as the categories of market data whose transparency could be governed by cryptographic frameworks. Unscrupulous or innovative traders can make use of the data provided by transparency. To demonstrate the hidden cost of transparency, we outline two common behaviors, one of which is immoral and the other parasitic: front-running and penny-jumping. We believe that these misappropriations of transparency are a contributing factor to the clash between dispersed market microstructures. Results that demonstrate transparency should increase liquidity and other specific results, such as this inquiry (Rindi, 2002). Front-running is unethical behavior in which a party with secret information about an upcoming large order to the market runs ahead of it to acquire a position in the hopes of generating a quick profit when the large order arrives. For example, if a broker learns that a mutual fund would buy a 10 million USD position in the stock, he or she may buy a lesser position at first, assuming that the common asset's purchase will raise the price. The possibilities for front-running and accusations related to it are endless.

Penny-jumping isn't illegal, although it's frequently referred to as "*parasitic*." This method extracts value from the market without adding any data. A dealer, for example, notices a large limit order on the order book and places a smaller limit order one tick above it. The penny-order jumpers

will be filled first, and he expects his potential gain to outweigh his potential loss because his disadvantage is mitigated by the larger limit order's free swapping option. When the market is unpredictably volatile, the stock will be exchanged at a higher price before the large order is filled. If the cost falls before it rises, the big order will be filled, and the penny jumper will lose a trick by leaving his position through the huge order (Donepudi et al., 2020). To address concerns about unethical and parasitic tactics, one solution is to create a market where only incomplete data is reported. In any case, it's uncertain if investors would trust the data's trustworthiness or market operators not to benefit from personal information. An unethical market operator could just fill a supporting party's offer before higher offers if the prices are disguised. To be sure, regulators have begun to impose openness to protect investors, citing the risk of financial gurus and brokers/traders profiting from secret market data.

There is additional evidence that data on large transactions being used. Huge blocks of stock are not shipped off the open market because of the risks of other brokers becoming aware of the block and selling in anticipation, potentially driving the price down, and because different dealers can exploit information on large orders in different unethical or unlawful ways (as mentioned above). Block trades are evidently carried out in "*higher up marketplaces*," where financial specialists search for the finest chance. The technique by which large blocks are shopped in the higher-up market has a big value influence on data leakage. The purpose of masking data in block trades is primarily to protect traders before a large trade occurs.

While these methodologies help to restrict the misuse of data they don't give any correctness guarantee and additionally, any published citations can be misused as in the past. These methodologies additionally necessitate that the block trades be isolated from the primary securities trades. This could have a critical effect on liquidity and generally market effectiveness.

Cryptographic Securities Exchange

A market operator in the Cryptographic Securities Exchange keeps a secret control book and provides a public version containing encrypted costs and amounts, as well as a history of its operations. Arriving limit orders are placed on the book or combined with existing limit orders; incoming market orders are combined with limit orders, and the operator verifies its actions. The main goal is to prevent unethical traders from abusing data in limit order books, putting traders who want to place a limit order at a disadvantage. Different dealers and market insiders (market makers, financial specialists, and trade workers) are among the enemies who attempt to profit dishonestly or parasitically by exploiting limited order data. The term "*partial transparency*" is used in trades that include three levels of pre-trading transparency in a market for a risky resource based on an open limit order book: full transparency allows agents to see the order flow and dealers' personal identifiers; half transparency allows them to see order sizes, and anonymity transparency allows them to only see order sizes. When it comes to current orders, the type of order is indicated; if it's in the book, it's a limit order. It's possible that the incoming orders are market or limit orders. In call barters, the exchange type (buy or sell) can be kept secret until the sale is completed; but, in constant double barters, it is unimportant to conceal whether an order is to buy or sell. Orders with a timed expiration are insignificant, as previously demonstrated.

Market makers can use these recent developments in encryption to create markets where this type of data can be buried and disclosed without revealing more information about basic orders. Data and accompanying verification are not required, and market designers may opt for delayed disclosure in many cases. Market designers can use the Cryptographic Securities framework to specify when market activity should be displayed and even create different disclosure criteria for different exchange sizes.

7-LAYER MODEL FOR CRYPTOGRAPHY FINANCIAL MARKET

A seven-layer model is shown in this section. Finance and cryptography are further classified in this paradigm, exposing five new areas of interest. The benefit of this architecture is that it can easily transition from technical to application, giving key stakeholders easy access. We can start at the top, with the Finance layer, and work our way down; this is a method of designing requirements and tracking them down to lower layers. If you're having a serious debate about a high-level application, this could be a good place to start. Alternatively, we can start at the bottom, with the Cryptography layer, then determine which toolkits to provide for the subsequent layers. We can develop our strategy to offering a wide range of alternatives to the wide-ranging financial applications layer by starting with more complex bottom levels.

Cryptography

At the bottom is Cryptography (Paruchuri, 2021), somewhat, the pure science area of cryptography tackles issues from a numerical perspective only, however, it delivers helpful properties, including:

1. Confidentiality - encryption algorithms
2. Integrity - hashes and message digests
3. Authentication – digital signatures, hash chains

Cryptography likewise can tackle extraordinary issues, when accurately formed (Vadlamudi, 2021) in Table 1.

Table 1
7-LAYER MODEL FOR CRYPTOGRAPHY IN FINANCIAL MARKETS

Layer	Description
Cryptography	Numerical methods to express certain truths that could be divided among parties for passing value.
Software Engineering	The tools to move guidelines over the net, and hold numbers and data dependably consistent on hubs.
Rights	A confirmation idea, with ownership designated to unit-value, and techniques for moving unit-values between unit personalities.
Accounting	A structure that contains value inside characterized and reasonable places.
Governance	Security of the framework from non-technical risks.
Value	Tools that deliver financial or other worth.
Finance	Applications for financial users, issuers of digital worth, and transactional and market operations.

Software Engineering

To take advantage of cryptography's features in a useful way, Software Engineering is required. We use information based theories (atomicity, value-based trustworthiness, and recovery) and network theories (feedback) to add qualities like dependability and robustness in the face of network and nodal instability, as well as planned inaccessibility in the case of smart cards and handhelds (Vadlamudi, 2020). Software Engineering provides us with a practical framework. We can talk about conveying something specific over an open network and be confident that the message will reach the intended receiver. We can know that the data received by the recipient is as desired by the sender thanks to the integrity techniques of the last layer. We can preserve the

integrity of communications throughout time by adopting specific arrangements of data set theories, even in the face of software and hardware failure.

Rights

With both cryptography and software engineering giving a network whereupon we can depend, we can consider sending messages that are intended for Financial Cryptographic purposes (Amin & Vadlamudi, 2021). In the Rights layer, we are searching for a method that equips a user with power over resources, in an unequivocal, definite style. Methods pointed toward accomplishing this include:

1. Identity-based frameworks, for example, those used by banks. Generally, such frameworks depend on the access (to a current account holder) of an account number and password that can access the user's account through an SSL-encrypted webpage.
2. Token Money that imitates the bearer cash tools with which customers are familiar.
3. Transport mechanisms for other payment frameworks, for example, the utilization of SSL-based frameworks to carry credit card data.
4. Hardware-based solutions, for example, smart cards.

Accounting

The previous layers provide techniques that are stable enough to be used for transmitting something of great value, such as rights. We currently require accounting methods to store and monitor rights over time. Accounting is a common topic for financial cryptographers, and it may have been tempting to neglect it, but experience shows that frameworks without common accounting functions lose their value with time. Double-entry accounting, asset reporting, and accounting conditions are examples of accounting discipline approaches. Accounting allows Financial Cryptography framework developers to create complicated frameworks that ensure that value is not lost as long as everyone respects the rules, and to quickly discover where the rules are not being followed. Rights, the layer above, defines what shall be displayed. Token cash, for example, is the simplest technique. A token-based or coin-based accounting system would necessitate a simple coin storage system for the user. The server would be more complicated, requiring an unissued value account, a float account, and a double-spend database linked to the float amount.

Governance

Once we have the assurance that the digital amount under management - the account-counting numbers - can be securely password-protected over the internet and stored on hubs, we must expand our vision to include hazards beyond the technical realm. The risk of fraud or misuse from parties who are trusted to deal with the framework occurs in any functioning innovation, whether it is trading or cash purchasing. This difficulty, referred to as the agency problem, can be solved through a variety of processes that we shall refer to as governance in this article.

Governance incorporates these procedures:

1. Escrow of significant value confided in third parties. For instance, funds underlying dollar money would be placed in a bank account.
2. Separation of powers: routine management from value creation, validation from accounting, systems from marketing.
3. Dispute resolution systems like intercession, assertion, ombudsmen, judiciary, and power.
4. Use of third parties for some part of the protocol, like the creation of significant value inside a closed system.

5. Auditing procedures that license external analysis of performance and resources.
6. Reports generation to keep data streaming to invested individuals. For instance, a user-driven display of the saved assets against which a currency is supported.

As technologists, we strive to make the conventions with which we deal as safe and self-contained as possible; our expertise is expressed by driving issue resolution into the lowest layers. However, this is an ideal to which we can only aspire; there will always be some value someplace that non-conventional means should be able to ensure. Our duty is made easier if we recognize the existence of this gap in the creative domain and attempt to close it using governance tools. The framework's goal is typically conveyed in a compromise between Governance and the lower layers: we accomplish what we can in the lower layers, and we clean up what we can't in Governance.

Value

We are now in a position to assign value to the structure, thanks to a framework that provides both inner and outside strength and security. By value, we mean the accounting unit, its meaning, and the range of appropriate amounts. A Value layer, for example, may assign any of the following to the virginal numbers of lower layers:

1. US dollars with an exchange scope of 25 cents as much as 500 dollars.
2. Bonds and stock, addressing tradable assets to raise capital.
3. Loyalty Points that can be granted for the acquisition of products.
4. Public products like huge loads of fish, or of public wastes, for example, huge loads of pollution.
5. Shares in virtual projects.
6. Funny money, being internal money for corporate meet ings.

Because the program is uninterested in this option, we could just use the product for another purpose - but the company must adhere to the security and cost recommendations. This layer is also known as the Contract layer because any value in an electronic structure represents a contract between the owner and the holder [35]. We plan the contract that formalizes the agreement between an Issuer and a client here.

Finance

Finally, we can build our application on top of the value layer, which provides structure to financial transactions. Because we're talking about financial cryptography, we'll refer to this layer as the Finance layer. We build an application that adds financial value to our goals in this section.

We construct all applications that can be immediately useful to users in the Finance layer. Consider the following example:

1. Retail trading including the acquisition of products.
2. Investment trading of securities.
3. Loyalty frameworks and Gift frameworks to support rehash business but not to fundamentally replace existing ways of payment.
4. Markets for the reasonable allocation of restricted public merchandise, for example, fishing zones or pollution.
5. Intermediation of Labor markets.
6. Closed or restricted purpose frameworks like shareware deals or corporate meeting accounting frameworks.

CONCLUSION

Close attention has been paid to cryptocurrencies in the literature, talking about whether they should disrupt the economy or are a speculative concept that could bite the dust or favor tax evasion and criminals. On the side of the first view, it is regularly contended they meet a market need for a quicker and safer payment and trade system, disintermediating monopolies, banks, and credit cards. Critics, then again, call attention to that the dramatic value of cryptocurrencies that makes them more of a speculative resource than another kind of cash. A key application of financial cryptography is providing regulated transparency of market data in securities exchanges, as well as evidence of accuracy (both of data and of market behavior). The convention presented here is simple to understand, well-aligned with current financial market patterns, and does not rely on sophisticated cryptographic natives that could undermine its use among traders. Finance research has begun to investigate the repercussions of varying levels of imperfect transparency, with the goal of ensuring liquidity and limiting abuse. Under partial transparency, cryptography can be utilized to demonstrate the proper action, as evidenced by the mentioned principles.

Similarly, the 7-layer architecture excels at coping with and reducing the inherent difficulties of Financial Cryptography. It accomplishes this by categorizing the field into seven distinct sections and providing an interconnecting method (layering). When a project is this layered, specialists in various controls may simply identify which sections are within their scope of expertise and which require distinct specialties. As a result, lawyers can see the Governance layer as their area of competence and give it the attention it deserves. Different layers can be treated as hidden elements, linking with necessities on the way down and up. Furthermore, developers can concentrate on Software Engineering and Rights, with Accounting taking precedence over Governance. A project manager in charge of delivering a Financial Cryptography framework will be able to track this down more effectively, given the model provides a unique agenda for coordinating the entire financial cryptography movement.

REFERENCES

Ahmed, A.A.A. (2020). Corporate attributes and disclosure of accounting information: Evidence from the big five banks of China. *J Public Affairs*. e2244. https://doi.org/10.1002/pa.2244

Amin, R., & Vadlamudi, S. (2021). Opportunities and Challenges of Data Migration in Cloud. *Engineering International, 9*(1), 41-50. https://doi.org/10.18034/ei.v9i1.529

Biais, B., Glosten, L., & Spatt, C. (2005). Market microstructure: A survey of microfoundations, empirical results, and policy implications. *Journal of Financial Markets, 8*(2), 217-264, https://doi.org/10.1016/j.finmar.2004.11.001

Donepudi, P.K., Banu, M.H., Khan, W., Neogy, T.K., Asadullah, ABM., & Ahmed, A.A.A. (2020). Artificial Intelligence and Machine Learning in Treasury Management: A Systematic Literature Review. *International Journal of Management, 11*(11), 13-22. https://doi.org/10.5281/zenodo.4247297

Madhavan, A. (2000). Market microstructure: A survey. *Journal of Financial Markets, 3*(3), 205-258, https://doi.org/10.1016/S1386-4181(00)00007-0

Maleque, R., Rahman, F., & Ahmed, A.A.A. (2010). Financial Disclosure in Corporate Annual Reports: A Survey of Selected Literature. *Journal of the Institute of Bangladesh Studies, 33*, 113-132. https://doi.org/10.5281/zenodo.4008320

Paruchuri, H. (2020). The Impact of Machine Learning on the Future of Insurance Industry. *American Journal of Trade and Policy, 7*(3), 85-90. https://doi.org/10.18034/ajtp.v7i3.537

Paruchuri, H. (2021). Conceptualization of Machine Learning in Economic Forecasting. *Asian Business Review, 11*(1), 51-58. https://doi.org/10.18034/abr.v11i1.532

Paruchuri, H., Vadlamudi, S., Ahmed, A.A.A., Eid, W., & Donepudi, P.K. (2021). Product Reviews Sentiment Analysis using Machine Learning: A Systematic Literature Review. *Turkish Journal of Physiotherapy and Rehabilitation, 23*(2), 2362-2368, https://turkjphysiotherrehabil.org/pub/pdf/322/32-2-316.pdf

Rindi, B. (2002). Transparency, liquidity and price formation. In: Proceedings of the 57th European Meeting of the Econometric Society (2002), Royal Economic Society.

Stoll, H.R. (2003). Market microstructure. Handbook of the Economics of Finance, in: G.M. Constantinides & M. Harris & R. M. Stulz (ed.), Handbook of the Economics of Finance, edition 1, volume 1, chapter 9, pages 553-604, Elsevier.

Vadlamudi, S. (2020). The Impacts of Machine Learning in Financial Crisis Prediction. *Asian Business Review, 10*(3), 171-176. https://doi.org/10.18034/abr.v10i3.528

Vadlamudi, S. (2021). The Economics of Internet of Things: An Information Market System. *Asian Business Review, 11*(1), 35-40. https://doi.org/10.18034/abr.v11i1.523

Vadlamudi, S., Paruchuri, H., Ahmed, A.A.A., Hossain, M.S., & Donepudi, P.K. (2021). Rethinking Food Sufficiency with Smart Agriculture using Internet of Things. *Turkish Journal of Computer and Mathematics Education, 12*(9), 2541-2551. https://turcomat.org/index.php/turkbilmat/article/view/3738

Zhu, Y., Kamal, E.M., Gao, G., Ahmed, A.A.A., Asadullah, A., & Donepudi, P.K. (2021). Excellence of Financial Reporting Information and Investment Productivity. *International Journal of Nonlinear Analysis and Applications, 12(*1), 75-86. https://doi.org/10.22075/ijnaa.2021.4659