OXFORD JOURNAL
OF STUDENT
SCHOLARSHIP

What is the Relation Between Bitcoin, Blockchain and Economic Growth?

Lucas Strapasson Blum
lucasstrapassonblum@gmail.com

ABSTRACT

Cryptocurrencies and Blockchain technology have transformed the discussion on digital finance, economic freedom, and economic development. While Bitcoin, the main object of study in this research, was created aiming at a decentralized alternative to the traditional financial system, its economic limitations continue to be debated, seeking to understand its potential role in the global economy. Using the Literature Review method of academic research, policy reports, and economic analyses, this research seeks to understand the current impact of Bitcoin and Blockchain on the economies where they have been implemented, the potential impact on the future of the financial system, how its economic limitations may affect an increase in the economic impact of this technology, and how it can be used in different areas in the future. After analyzing the selected articles, the results suggest that Bitcoin and Blockchain have a positive impact on the economic growth of certain countries with small economies that have adopted cryptocurrency. However, this impact is relatively small and very different depending on the country studied. Due to economic limitations such as the cost of security, it may not have a greater influence on larger economies.

Nevertheless, looking to the future, the potential of Blockchain and Bitcoin is in their possible implementation in the traditional financial system in various ways, from regulation and integration into the SWIFT system to governmental use, such as Blockchain being used in public administration, ensuring greater efficiency and speed of use.

KEY WORDS - Bitcoin, Blockchain, GDP, Economic Growth, Cryptocurrencies, Trusted Party.

1: INTRODUCTION: FOUNDATIONS OF BITCOIN AND BLOCKCHAIN

In 2008, an anonymous person/group, operating under the name Satoshi Nakamoto, published a white paper titled "Bitcoin: A Peer-to-peer Electronic Cash System." This article explains the main concepts of Bitcoin and its transaction system behind it, the Blockchain, and finally, proposes a revolutionary idea for the economic system: a decentralized system of financial transactions without an intermediary and entirely digital.

Since its creation, Bitcoin had an extraordinary growth. From not being relevant in its first years, Bitcoin reached a total market capitalization of over one trillion dollars at its peak, attracting the attention of investors, institutional players, governments, and academic researchers. The Blockchain technology, at the same period of time, expanded beyond digital currencies, being used in different areas as supply chain management, healthcare, intellectual property, public administration, and decentralized finance (DeFi). What began as an experiment has evolved into a global technological and economic revolution, generating academic studies about its implications for economic growth.

Despite its growth, the relationship between Bitcoin, Blockchain, and economic growth remains a debate. Supporters argue that these technologies can promote financial inclusion, generate smaller transaction costs, increase economic efficiency, and provide alternative monetary systems for countries with unstable currencies or underdeveloped financial infrastructure. Critics, however, point to limitations as volatility, high energy consumption, security vulnerabilities and regulatory uncertainty. The case of El Salvador, which became the first country to adopt Bitcoin as legal tender in 2021, shows us the complexity of integrating cryptocurrency into a national economy.

This research aims to investigate whether Bitcoin and Blockchain have an impact on the economic growth of the countries that have been using them, and how governments have implemented them. To this objective, it employs a Literature Review methodology, systematically analyzing academic papers, policy reports, and economic analyses. Sources were selected based on four criteria: direct relevance to Bitcoin, blockchain, or cryptocurrency adoption; publication in peer-reviewed journals, recognized institutional working papers (NBER, IMF), or accredited university theses; publication primarily between 2015 and 2026, with the exception of essential foundational works such as Nakamoto (2008) and Kiyotaki and Wright (1991); and availability in English. Journalistic articles, opinion pieces, and non-peer-reviewed sources were excluded, with the exception of official institutional communications directly relevant to the topics discussed. Literature was gathered through Google Scholar, SSRN, and the NBER repository, using search terms including "Bitcoin economic growth," "blockchain adoption," "cryptocurrency GDP," and "Nakamoto trust," among others. The final selection comprises approximately 50 sources spanning empirical studies, theoretical models, case studies, and institutional reports. The review is structured into four sections: an analysis of current economic developments and prospects; a discussion of economic limitations, focusing on Nakamoto Trust and the cost of security; an examination of expectations for the future impact of Bitcoin and Blockchain; and a concluding synthesis. Before addressing these themes, it is necessary to establish the key concepts and foundations of the technology: transactions, proof of work,

and Bitcoin mining and reward.

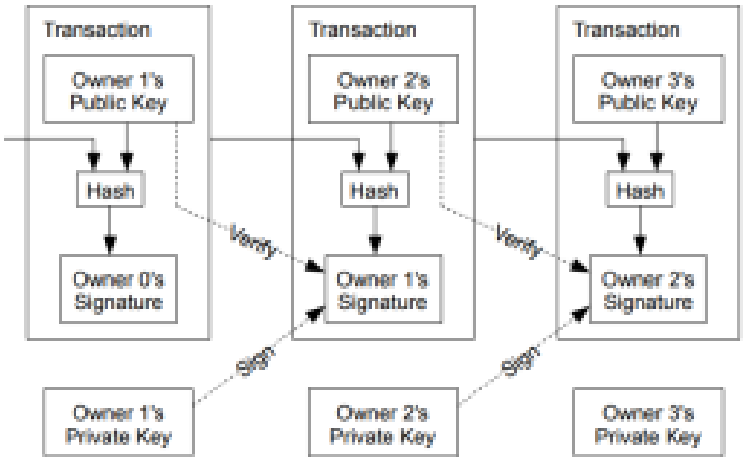
While the literature review methodology allows a synthesis of existing research, several limitations must be acknowledged. Publication bias may lead to an overrepresentation of studies with positive findings, potentially overstating the economic impact of Bitcoin and blockchain. English-language bias restricts the scope of the review, as relevant studies published in other languages. Additionally, the rapid pace of development in the cryptocurrency space means that some findings may become outdated relatively quickly. Finally, the heterogeneity of methodologies across reviewed studies, ranging from econometric models to qualitative case studies limits the degree to which findings can be directly compared.

1.01: TRANSACTIONS

The transaction is the fundamental mechanism by which value is transferred between participants in the network. According to Nakamoto's explanation in the original white paper, "an electronic coin is a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership" (Nakamoto, 2008). This means that ownership of Bitcoin is not stored in an account in the traditional sense, but rather encoded in a continuous chain of cryptographic proofs that links every transaction back to its origin. Unlike traditional financial systems, ownership in Bitcoin is not stored in centralized accounts, but in a continuous chain of cryptography that links each transaction to its history.

When it is added to the network, a transaction does not immediately become permanent. It first enters a waiting area named Mempool (memory pool), before a miner selects it to be included in a new block. Miners usually prioritize transactions that offer better fees. When a block containing the transaction is mined and added to the Blockchain, the transaction receives its first confirmation. With each subsequent block added on top, the transaction becomes increasingly difficult to reverse, eventually reaching a practical irreversibility. This process guarantees that the Bitcoin network can operate without a central authority, using, instead, cryptographic proof and economic incentives. The main components of a transaction include the sender's address, the receiver's address, the transferred amount, and a cryptographic signature. These addresses function similarly to account numbers, while the signature, generated using the sender's private key, ensures that only the owner can authorize the transfer. Additionally, the signature secures the transaction data, preventing any modification.

This process is illustrated in Nakamoto's original diagram, where each transaction is represented as a link in a chain of ownership transfers. In the figure, each owner signs the previous transaction using their private key and transfers the value to the next owner's public key. The arrows labeled "sign" and "verify" demonstrate how each transaction is both authorized by the sender and verifiable by others in the network. This structure makes the system transparent and secure, as every transfer can be independently validated without relying on a central authority (Nakamoto, 2008).

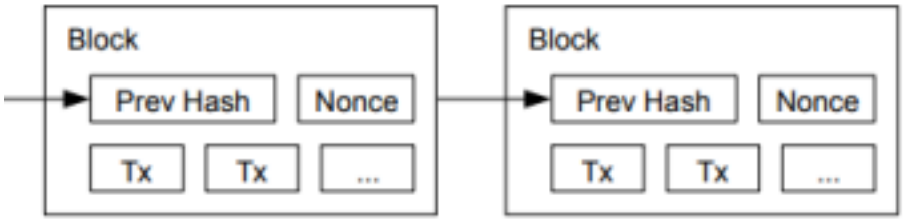


1.02: PROOF OF WORK, BITCOIN MINING AND REWARD

In the traditional financial system, people deposit their money in a bank, and investors invest in a country. But why? The answer, in this case, is simple: these people trust the bank and the country. This is the basis of the current financial system: trust in a trusted third party. Because the Bitcoin ecosystem is completely decentralized and has no third party, the traditional trust system does not apply.

In the Proof of Work format, participants known as bitcoin miners validate transactions by solving complex computational problems. More specifically, miners try to find a value called a nonce that, when combined with the block's data and processed through a hash function, produces a result that meets certain requirements.

As shown in Nakamoto's original diagram, each block includes the hash of the previous block, forming a chain. This structure, according to Nakamoto, makes the system secure, since changing a single block would require redoing the work for all the blocks that come after it.



Bitcoin mining is the process through which these blocks are validated and added to the blockchain. As a reward for their work, miners receive newly created bitcoins as well as transaction fees. This reward system is important because it motivates participants to maintain the network, replacing the need for a central authority.

However, Proof of Work also has important limitations, that will be explained in more detail in Section 3: "Nakamoto Trust and Economic Limitations of Bitcoin."

2: ECONOMIC DEVELOPMENTS AND PROSPECTS

Although Bitcoin had a small relevance in its early years of existence and participation in the economy, it has, in recent years, begun to be used in a structured and institutionalized way by several countries around the world, in different ways and with different outcomes. This section analyzes the impact and relationship between Bitcoin, Blockchain, and economic growth across different countries, and how it was adopted in each case. The main examples are El Salvador (the first country to adopt the cryptocurrency as legal tender), Bhutan, African countries such as Zimbabwe and Nigeria, and Asian countries such as China, Japan, India, and Singapore. To analyze the impact, the conclusions and calculations from different articles and research papers will be discussed, each generally focused on a specific country.
This section begins by briefly explaining certain topics that directly or indirectly contribute to the economic growth of countries that adopt the cryptocurrency. After this explanation of the economic concepts, the Bitcoin adoption cases of each country will be analyzed, concluding if the technology had an impact on the economy in any form.

2.01: THEORETICAL CHANNELS

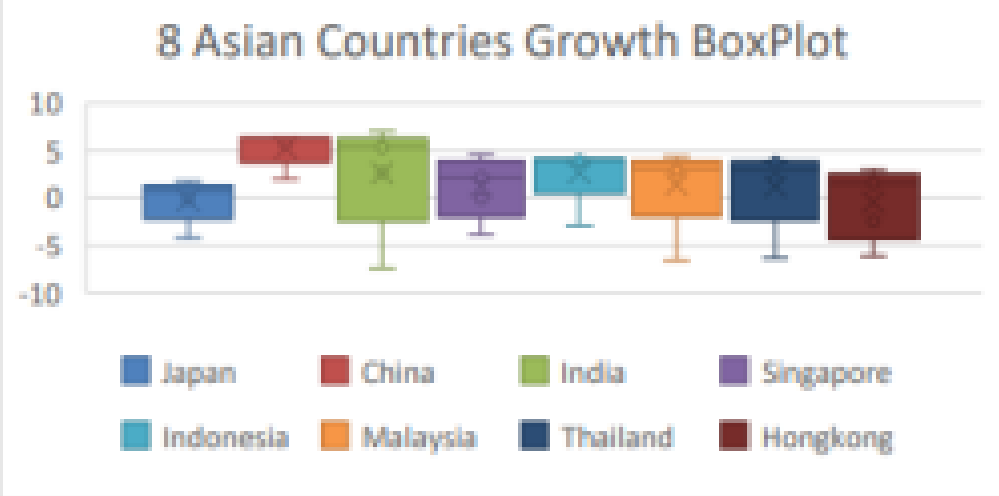
The relationship between Bitcoin, blockchain technology, and economic growth can be understood through several key economic mechanisms. One of the most relevant channels is the reduction of transaction costs. By eliminating the need for intermediaries such as banks and payment processors, blockchain systems allow for faster and cheaper transactions, particularly in international transfers. This reduction in costs can improve efficiency in financial systems and facilitate economic activity.

Another important mechanism is financial inclusion. In countries with smaller banking systems, cryptocurrencies can provide access to financial services for individuals who are excluded from traditional institutions. By enabling peer-to-peer transactions through digital infrastructure, Bitcoin has the potential to expand participation in the financial system.

In addition, blockchain technology may create transparency and trust in economic interactions. Instead of trusting only on centralized institutions, trust is established through cryptographic verification and decentralized consensus mechanisms. From an economic perspective, this represents a change from institutional trust to a system based on verifiable rules, which may reduce inefficiencies and increase reliability in certain contexts.

Finally, there is another crucial concept explained in the article "Bitcoin on Economic Growth (Case of 8

Asia Countries)" (Titalessy & Situmeang, 2024). This economic concept is named Growth Elasticity, which will be used in the calculations of Bitcoin's economic impact in different Asian countries. The elasticity of economic growth shows the country's ability to maintain the stability of its economic growth. The lower the growth elasticity, the more stable the economic growth. Elasticity is obtained from the standard deviation value of economic growth data.



The boxplot above displays the distribution of annual GDP growth rates (%) for each of the eight countries studied over the period 2011–2016. The vertical spread of each box reflects the variability of growth across years, and is used to compute each country's growth elasticity, defined as the standard deviation of its annual GDP growth rates. A narrower box indicates more stable, predictable growth, while a wider box reflects greater volatility. China presents the lowest elasticity (1.66), meaning its annual growth rates remained tightly clustered around a high mean, consistent with its managed economic model during this period. Japan (2.09) and Indonesia (2.77) follow as the next most stable economies. At the other extreme, India records the highest elasticity (5.23), reflecting significant fluctuations in annual growth, followed by Malaysia (4.07), Thailand (3.88), and Hong Kong (3.43) (Titalessy & Situmeang, 2024).

2.02: CASE STUDIES AND EMPIRICAL EVIDENCE

This subsection analyzes the impact of Bitcoin and Blockchain adoption by the population and/or governments of various countries on their economies, based on a literature review of several published articles, while also examining the calculation models used by the authors to study this impact. First, the models used in the articles will be explained, followed by an analysis of each country's case separately.

Firstly, P. B. Titalessy and R. J. Situmeang (Titalessy & Situmeang, 2024), the authors of the article cited earlier, used the following model to examine whether cryptocurrencies influence economic growth. In this equation, EG represents economic growth (the dependent variable), while the remaining variables

represent Internet access (I), labor (L), capital (K), and technology (T):

EGit = β0 + β1(BTC) + β2(I) + β3(L) + β4(K) + β5(T)

Table 1. Descriptive Statistics Example

Indicator	BTC	L	K	T	I	EG
Mean	23.269.884,93	191.687.635	1.066.946.351.045,76	31,28	67,24	1,72
Maximum	838.940.296,25	792.758.868	6.410.859.610.479,94	69,65	93,18	6,98
Minimum	0,0001	3.472.519	65.682.076.006,81	7,36	16,5	-7,48
Standard Deviation	132.736.014,49	274.016.492	1.853.153.221.621,35	20,08	24,66	3,88
Kurtosis	39,4	0,43	3,51	-1,3	-0,83	0,23
Skewness	6,26	1,4	2,2	0,4	-0,69	-1,04
Obs.	40	40	40	40	40	40

“The results presented in table 1 indicate that both capital and Bitcoin have positive coefficients, although the coefficient for capital is significantly larger. Specifically, a 1 percent increase in Bitcoin usage increases economic growth by approximately 0.043926, while a 1 percent increase in capital increases economic growth by approximately 2.444085” (Titalessy & Situmeang, 2024). A very similar formula was also used in the research "The Influences of Cryptocurrency on Economic Growth: Case Study of Bitcoin in Five Asian Countries (2011–2016)" (Utomo, 2018), highlighting its importance in the analysis of bitcoin’s economic impact.

As analysed by P. B. Titalessy and R. J. Situmeang, the results show a positive relationship between Bitcoin and GDP, indicating that cryptocurrencies have a positive impact on economic growth. However, the impact of Bitcoin on economic growth is not yet as big as the capital. From that perspective, it can be analysed that Bitcoin does not have yet economic relevance or infrastructure comparable to capital (K) and, as a result, has a significantly smaller impact on economic growth.

Asian Countries - Japan, China, India, Singapore, Indonesia, Malaysia, Thailand, and Hong Kong are the countries referenced in the chart and article cited above. According to the authors of "Bitcoin on Economic Growth (Case of 8 Asia Countries)" (Titalessy & Situmeang, 2024), as already described, Bitcoin has a positive impact on the economy of all 8 countries studied. However, this value is not comparable and does not have the same economic relevance as capital. The conclusion that Bitcoin was positive in these cases can be drawn from the reasoning present in the authors' conclusion, where they affirm that openness to technological innovation by all related institutions as companies and governments is important, and that regulation may be crucial, requiring the use of the technology with safety and responsibility.

The findings of Titalessy and Situmeang (Titalessy & Situmeang, 2024) reveal that both Bitcoin and capital have positive coefficients in the regression model, however, capital's effect is substantially larger. Concretely, a one percent rise in Bitcoin usage corresponds to an increase of approximately 0.044 in economic growth, compared to approximately 2.44 for a one percent rise in capital. These results confirm that while Bitcoin does contribute positively to economic growth across the eight countries studied, its influence remains far smaller than that of conventional capital investment.

Bhutan - Although Bhutan is a country with a small population and a relatively smaller GDP compared to the other countries cited in this research, it is the country where Bitcoin has the greatest impact. While in other countries Bitcoin had a positive but much smaller impact on economic growth than capital, in Bhutan, Bitcoin holds reserves approximately 40% of GDP (Adhikari, 2026). This is due to the way Bitcoin was adopted: Bhutan uses its surplus energy production to mine Bitcoin, and uses the mining reward, as explained earlier in subsection 1.02 as a form of value reserve. Therefore, the way in which cryptocurrency is adopted by each country greatly influences the economic impact generated.

El Salvador - El Salvador, however, does not present an impact similar to the other countries. Although it was the first country in the world to adopt Bitcoin as official currency alongside the US Dollar, public adoption did not reach the levels expected by President Nayib Bukele, a prominent cryptocurrency enthusiast, according to the research article "Perceptions of Bitcoin adoption and its socio-economic implications: financial inclusion, social trust and governance in El Salvador" (Pumcharoen, 2024). Based on Phutanet Pumcharoen, author of "The Impact of Bitcoin Adoption on Economic Growth: An Empirical Case Study of El Salvador" (Kiyotaki & Wright, 1991) the primary finding of the empirical analysis is that Bitcoin adoption had a significant negative impact on FDI across all three econometric methods employed (ITS, OLS, and VAR) with an estimated net FDI outflow of approximately 350 million USD under ITS and OLS, and a 2.6% decline in the VAR model. Regarding GDP growth, the ITS and OLS models found no statistically significant effect, suggesting that Bitcoin adoption did not meaningfully alter El Salvador's economic output in those frameworks. However, when applying the VAR model, the results indicate secondary positive associations: a 5.98% positive impulse on GDP growth, an 8.5% positive effect on remittance growth, and a 6.6% reduction in the unemployment rate, all significant at the 1% level. Pumcharoen notes that these VAR findings are consistent with existing literature, though the overall picture remains mixed, with foreign investment declining while certain domestic indicators showed improvement.

Taken together, the cases examined in this section suggest that the economic impact of Bitcoin adoption is not determined by the technology itself, but by the structural conditions it is introduced in. Bhutan and the eight Asian countries studied by Titalessy and Situmeang represent cases where Bitcoin operated as a complementary economic tool, either leveraged strategically alongside existing energy infrastructure as in Bhutan, or absorbed gradually into digitally connected economies, as in the Asian case. El Salvador, however, represents a case of top-down institutional adoption without the preconditions necessary for organic absorption, such as financial infrastructure and public trust. The contrast between these cases implies that Bitcoin's contribution to economic growth is conditional on at least three factors: the existence of a strategic adoption model rather than broad legal mandate, a degree of technological and

financial infrastructure capable of supporting integration, and an institutional environment that does not generate negative signals to foreign investors. In the absence of these conditions, Bitcoin adoption may produce mixed or even negative macroeconomic outcomes, regardless of its theoretical potential.

2.03.: SUMMARY AND DISCUSSION

Existing literature gives mixed evidence about the economic impact of Bitcoin and blockchain. Several studies suggest that blockchain adoption can improve efficiency in financial systems by reducing processing times and operational costs, particularly in cross-border payments. Other research discusses the potential of distributed ledger technologies to support innovation in digital economies, contributing to new business models and financial services.

These findings demonstrate the important role of capital in economic development while also suggesting that Bitcoin may contribute positively to economic growth. However, its impact remains significantly smaller than that of traditional economic drivers such as capital investment. The economic impact of Bitcoin varies considerably across countries, as illustrated by the contrasting cases of Bhutan, where Bitcoin mining accounts for an estimated 40% of GDP due to the strategic use of surplus hydroelectric energy (Adhikari, 2026), and El Salvador, where the overall economic impact has been mixed despite Bitcoin's status as legal tender. This difference can be explained by several factors, including levels of public adoption, financial infrastructure, and overall market conditions.

The literature also emphasizes important limitations. Some studies argue that the direct impact of cryptocurrencies on macroeconomic growth remains limited, as their use is still relatively restricted compared to traditional financial systems. Additionally, concerns related to volatility, regulatory uncertainty, and technological constraints are frequently cited as barriers to broader economic impact. Overall, the current body of research suggests that while blockchain technology holds significant potential, its contribution to economic growth is still conditional on adoption levels and institutional factors.

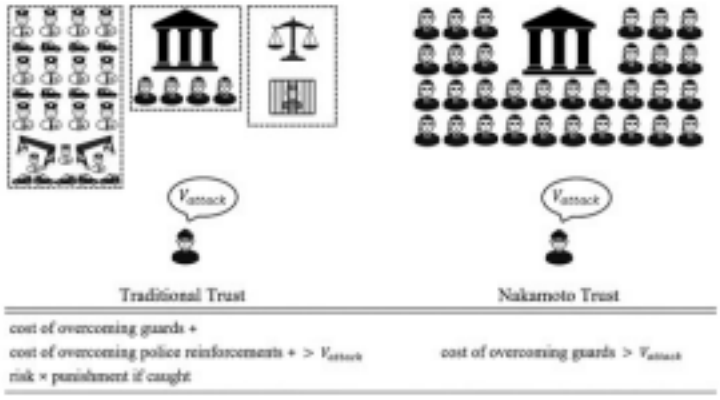
Finally, based on the conclusions of these studies, Bitcoin seems to have a positive impact on GDP growth in the majority of the countries analyzed. However, important nuances must be considered: despite the impact being positive in most cases, there is significant variation in magnitude across countries, showing the importance of context factors such as infrastructure, market size, and public adoption. Moreover, it can be concluded that while the results indicate a positive relationship between Bitcoin and economic growth, the significantly smaller coefficient compared to capital suggests that Bitcoin functions more as a complementary factor than a primary driver of economic development.

3: NAKAMOTO TRUST AND ECONOMIC LIMITATIONS OF BITCOIN

As previously explained, Bitcoin operates in a decentralized manner, meaning without the presence of a third-party intermediary. Even in his book "The Wealth of Nations," Adam Smith argues that the role of

the state in the economy should be minimal, but not nonexistent, as do several famous economists such as Friedrich Hayek and Milton Friedman. Satoshi Nakamoto, however, presented a revolutionary and ingenious system where the existence of a regulatory body does not exist and, according to Nakamoto, is unnecessary. Nevertheless, this system presents serious economic limitations, which will be analyzed in this section.

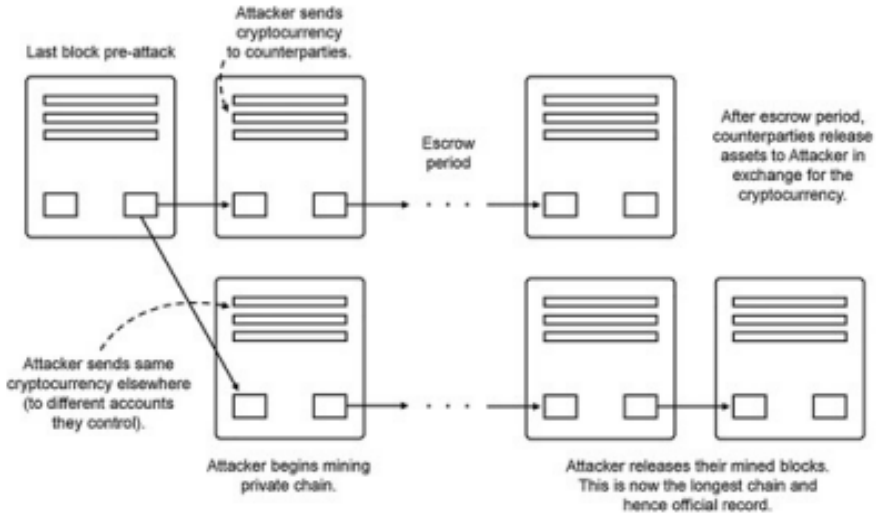
As author Eric Budish illustrates in his article "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchain" (Budish, 2025), a criminal thinking of robbing a bank must consider how many security guards he will need to overcome, that the bank may call the police, and that if caught, he will go to jail. Similarly, a country considering whether to invade another must consider not only the soldiers at the border but also military reinforcements and the possibility of a counterattack (an analog of Becker's deterrence from courts). In contrast, the Nakamoto model relies only on having a very large number of security guards at the bank or soldiers at the border, which, in Nakamoto's system, are the Bitcoin Miners. This works, but it is very expensive and scales poorly with the stakes involved.



As Budish concludes, in the traditional model there are two sources of scale economies. First, the police do not need to be present at a particular bank to provide security, as they can protect many locations at the same time, as long as they are not all attacked at once. Second, the courts can deter crime through the credible threat of prosecution and imprisonment, in other words, a fixed-cost investment in judicial capacity can deter a large quantity of potential criminal activity. This is the essence of the model of optimal deterrence, and is central to Hayek's resolution of the paradox that freedom requires a government with the power to coerce (Budish, 2025).

Another concerning economic limitation is the double-spending attack, a vulnerability that Nakamoto himself acknowledged in his original white paper. In essence, double-spending means spending the same cryptocurrency more than once. Basically, falsifying transactions and generating a structural problem in the blockchain. As the Bitcoin system is decentralized, an attack on the permissionless blockchain chain requires only that the attacker control 51% of the entire computational power of the system, meaning more computing power than all Bitcoin miners combined. If that quantity of power were concentrated in a single actor, all that would be needed to execute an attack is the creation of an alternative chain. As

Budish exemplifies, In a double-spending attack, the attacker first conducts normal transactions on the public chain, receiving goods or assets in exchange. Simultaneously, however, the attacker secretly constructs an alternative chain that hides those transactions, redirecting the funds to accounts under their own control. Once the escrow period lapses and the goods are received, the attacker releases the alternative chain, ending up with both the transacted goods and the original cryptocurrency.The following illustration exemplifies this process. (Budish, 2025).



Another point that exposes a further economic limitation of the permissionless blockchain is what Budish calls "Specific Capital and Collapse." In this hypothesis, the researcher analyzes the possibility of Bitcoin becoming more economically important, being used by a much larger number of individuals and, especially, corporations. If a company holds a financially significant amount of cryptocurrency and its value has a significant decrease, the company would be negatively affected and, depending on the magnitude of the loss, potentially going to bankruptcy. If this scenario becomes real, it is possible that an attack on Bitcoin could be motivated not by immediate monetary profit, but by a so-called "kamikaze attack," where the main goal is to devalue the currency in order to financially harm another person or company. This concern has grown in recent years for two main reasons. Firstly, Bitcoin currently holds greater economic relevance than it did during its early years, when its value was negligible and it was even used to purchase a pizza. If the appreciation trend that has persisted since its creation in 2008 continues, more companies will begin making more substantial investments in the crypto market. If this trend comes to reality, it leads to the second reason: the existing interest in harming certain companies. As previously described, if companies come to hold a significant monetary value in crypto assets, an attack focused on only causing a collapse becomes attractive to actors who would benefit, in any way, from the financial difficulties or bankruptcy of the affected company.

Eric Budish also substantiates his critique of the Bitcoin system using three equations in Section III of his article, grounding the analysis of the risks of permissionless blockchain described above. Following this, he applies a Nash equilibrium solution in a one-shot game and, finally, contrasts the result with the trust system of the traditional financial system.

Equation 1 — Zero-Profit Condition

The first equation addresses how much "trust support" such as computational work or stake that honest participants will provide. Budish assumes a competitive market with free entry. Miners enter the system while profits are positive and exit when profits turn negative. In equilibrium, profits are zero. Formally:

N*c = p_block

Where N* is the total quantity of trust support, such as computational power; c is the cost per unit of support, including electricity and capital equipment costs; and p_block is the reward paid to the miner who successfully adds a block. In short, the total spent by honest miners (N*c) is exactly equal to the total reward distributed by the protocol (p_block). This follows the standard logic of a rent-seeking tournament, in which the prize is dissipated by the costs of competition.

Equation 2 — Incentive Compatibility Condition (Majority Attack)

The second equation focuses on how much security the honest trust support actually produces. The central vulnerability of the Nakamoto blockchain is the majority attack: any agent controlling more than 51% of the total computational power can rewrite the transaction history. For the network to be secure, it must be unprofitable for a potential attacker to acquire such a majority. Budish models an outside attacker who must acquire A·N* units of trust support, where A > 1, at a cost of A·N*·c per unit of time, over the expected duration of the attack t(A). The security condition is:

A* · N*c · t(A*) > V_attack

Where A* is the attacker's optimal computational power multiplier, t(A*) is the expected duration of the attack, and V_attack is the economic value of the attack, which means how much the attacker can steal through double-spending. From this condition, Budish concludes that for the system to be secure, the gross cost of conducting the attack must exceed its benefit. The key issue is that both the attacker's cost and the honest miners' cost depend on the same term N*c, which is precisely what makes the two equations linkable.

Equation 3 — Equilibrium Constraint

For his third equation, Budish examines what equations (1) and (2) imply when combined. Since N*c appears in both previous equations, he combines them directly:

p_block > V_attack / (A* · t(A*))

In other words, the per-block payment to honest miners must be large relative to the benefit of an attack. This is Theorem 1 of the article and the central result of the section. Using these equations, Budish

calculates that, in the base case with a one-hour escrow period, maintaining the security of the network costs 5% of the value at risk per block. This is equivalent to 720% per day or 263,000% per year. To protect the system against a $40 billion attack would require an annual security expenditure equivalent to the entire global GDP in 2023. In light of these facts, the cost of Nakamoto trust is extremely expensive in absolute terms relative to the stakes involved, and its expense grows linearly with the stakes.

The economic reading of this model is not only concerning but also devastating: imagine if every user of the Visa network had to pay, every ten minutes, a fee proportional to the value of a successful attack on the entire Visa network, or that the security of a bank depended only on how many guards it has at this very moment, rather than on the possibility of arrest or police intervention. This is exactly what Nakamoto Trust imposes.

The One-Shot Nash Equilibrium Game (Section III.E)

To make the argument more rigorous, Budish also presents a version of the model as a static Nash game, in which players simultaneously choose how much trust support to allocate and whether to attack or play honestly. The results shown in Lemmas 1 and 2 and Proposition 2 (Budish, 2025) reach the same conclusion as the three equations: in the limit with many players, the compensation required to sustain an honest equilibrium must exceed the value of an attack, confirming equation (3).

Synthesizing the three limitations analyzed in this section (cost of security, vulnerability to double-spending attacks, and the risk of Specific Capital and Collapse) it can be concluded that the economic constraints of the permissionless blockchain are not independent weaknesses, but structurally interconnected. The cost of security, as formalized by Budish's equilibrium constraint, scales linearly with the economic value at stake, making the system progressively more expensive to maintain as adoption grows. This same dynamic amplifies the incentive for double-spending attacks at higher value thresholds, since the potential gains increase alongside the network's economic significance. The Specific Capital and Collapse scenario then represents the endpoint of this trajectory: a system whose security costs are prohibitive, whose attack incentives grow with adoption, and whose increasing integration into corporate balance sheets introduces non-monetary motivations for destabilization. Together, these limitations suggest that the permissionless blockchain faces a fundamental scaling paradox: the conditions required for broader economic relevance are precisely the conditions that render the system most vulnerable. This does not preclude a future role for blockchain technology, but it does imply that such a role will likely require departing from Nakamoto's original permissionless architecture, a point that connects directly to the institutional and hybrid models discussed in Section 4. Based on this economic analysis, it can be concluded that the permissionless blockchain system created by Nakamoto, which governs the entire structure of Bitcoin, presents serious economic limitations and security vulnerabilities that, in its current form, present significant limitations to a bigger adoption in the global financial system.

4: EXPECTATIONS FOR BITCOIN AND BLOCKCHAIN'S IMPACT IN THE FUTURE

Through the Literature Review methodology applied in the preceding sections, it was possible to understand the foundational concepts of Bitcoin and Blockchain, analyze adoption cases across various countries, and examine the economic limitations that constrain a broader use of the permissionless blockchain envisioned by Nakamoto. With this in mind, a central question emerges: based on the conclusions drawn in the previous sections, what might be the future of cryptocurrency and the Blockchain system in the financial market? This is the central question of this section, which, drawing on academic articles, research papers, and reports related to these technologies, seeks to understand the possible future trajectory of Bitcoin and Blockchain. In essence, the future of Bitcoin and blockchain will depend less on their original decentralized architecture and more on their ability to operate within institutional and regulatory frameworks.

4.01: BITCOIN: INSTITUTIONAL ADOPTION AND ETFs

As established in Section 3, Bitcoin and the permissionless blockchain system present economic limitations that prevent large-scale adoption in their current form. Nevertheless, it remains entirely possible that Bitcoin could be adopted in different ways. One of the most significant pathways is its integration into financial markets through Exchange-Traded Funds (ETFs). A Bitcoin ETF offers a greater sense of security than holding the cryptocurrency directly, enabling a broader audience to gain exposure to Bitcoin without the need to purchase or store it themselves.

According to the authors of "The Impact of Bitcoin ETF Approval on Bitcoin's Hedging Properties Against Traditional Assets," there is an extensive debate regarding Bitcoin's safety as a financial asset. While supporters classify it as a safe-haven asset and refer to it as "digital gold," skeptics argue that its high volatility and low liquidity prevent it from being reliable, characterizing it as purely speculative. The approval of Bitcoin ETFs, however, represents a significant structural change that may help resolve these debates by bringing greater confidence, transparency, and security, and by potentially reducing the risks for investors. This development is also particularly relevant given the economic limitations discussed in Section 3: it suggests that regulation, or the existence of a regulatory entity — as BlackRock has already begun to establish — may be the only viable path for Bitcoin to achieve a greater economic relevance and impact.

Based on the reviewed literature, it can be concluded that ETFs represent a significant step toward the integration of Bitcoin into the traditional financial system. However, this institutionalization also raises an important counterpoint: the increasing centralization of the system. This shift is uncomfortable for many cryptocurrency enthusiasts, as institutional adoption was not the future Nakamoto envisioned, and it contradicts the original philosophy of Bitcoin. This represents a fundamental paradox: while Bitcoin was designed to eliminate intermediaries, its mainstream adoption increasingly depends on traditional financial institutions. Furthermore, this centralization may reduce the systemic resilience that Bitcoin

originally aimed to provide.

4.02: BLOCKCHAIN IN PUBLIC ADMINISTRATION

Blockchain, on the other hand, can be considered more promising than Bitcoin itself. It presents numerous possibilities for adoption even outside the financial market, suggesting a broader potential societal impact. One of the most relevant applications is in public administration, as analyzed by M. Kassen in the article "Blockchain and Public Sector Innovations: Understanding Decentralized Models of Technology Adoption in E-government." According to the author, blockchain technology can provide greater transparency and efficiency in government operations. Kassen highlights that this model offers a foundation for stakeholders including policymakers, technologists, and civil society to design blockchain-based systems that are not only efficient but also inclusive and legitimate.

Blockchain therefore holds potential for diverse applications in public administration, including transparency and anti-corruption measures, environmental monitoring, shared data management, public procurement, and digital identity and public records. While the author emphasizes that blockchain adoption must be approached with caution and further analysis, the evidence points to significant potential for this technology well beyond the financial sector. It must be noted, however, that an important counterpoint exists: the adoption of blockchain in the public sphere depends heavily on state capacity and institutional readiness, and may not deliver the expected benefits if not implemented correctly.

4.03: BLOCKCHAIN AND THE SWIFT SYSTEM

A major opportunity for blockchain lies in its potential adoption within global transaction systems, particularly the SWIFT network. SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a secure global financial messaging network connecting more than 11,000 banks and institutions across approximately 200 countries. As the world's primary financial transaction network, the adoption of blockchain technology within it could represent a new era for both blockchain and related crypto assets.

According to an announcement published on SWIFT's own website, in September 2025, the network announced an initiative to integrate a blockchain-based shared ledger into its core infrastructure, enabling 24/7, real-time cross-border settlement and tokenized asset transactions. Working with over 30 global banks, this move transitions SWIFT from a messaging system to a platform for direct value settlement, connecting traditional finance with digital ecosystems across the world.

This development, while still in its early stages, demonstrates the potential benefits that can arise from blockchain technology when applied in an adapted and institutionalized form. According to the authors of "Impact of Fintech Innovation on Cross-border Payments: SWIFT vs. Blockchain," blockchain already presents itself as a strong alternative for cross-border transactions. The researchers conclude that while SWIFT remains a dependable choice due to its established infrastructure and global reach, blockchain presents a compelling alternative by reducing intermediary involvement and potentially decreasing

transaction costs. They also note, however, that the adoption of blockchain within the SWIFT system could represent a significant shift in the current paradigm of financial transactions. Despite the risks involved, including concerns about achieving adequate scalability, a careful and gradual transition could yield substantial benefits, as also analyzed by Bayram, Talay, and Nur Kutlu.

This adoption is ultimately crucial for the blockchain system itself. As discussed in Section 3, the cost of Nakamoto trust scales with economic value, making fully decentralized systems unlikely to dominate global finance. Instead, hybrid or institutional models are more viable, and the SWIFT integration represents precisely this kind of model.

4.04: GENERAL FUTURE OF BITCOIN AND BLOCKCHAIN

Beyond the sectors discussed above, the future of blockchain more broadly presents enormous potential. As stated by D. Levis, F. Fontana, and E. Ughetto in "A Look into the Future of Blockchain Technology," blockchain technology is likely to change the financial services sector and the broader economy, despite its current immaturity and the technical, economic, and regulatory challenges it faces [40]. Through the Delphi method, the authors map out the applications of blockchain and its future expectations, finding that this system has become increasingly economically relevant, with a 24% growth in the use of blockchain and cryptocurrencies, driven primarily by its role in fintech and decentralized finance (DeFi). As the world broadly adopts blockchain-based technologies, this technology is expected to continue growing and supporting economic innovation and integration, albeit in a form different from that originally envisioned by Nakamoto. As the authors conclude, the decentralized structure of blockchain has facilitated the development of a variety of real-time businesses, and future applications of blockchain technology are almost limitless [40]. More broadly, it is likely that blockchain will increasingly be implemented in sectors where its advantages are significant and outweigh its structural limitations.

4.05: DISCUSSION AND CONCLUSION OF SECTION 4

In light of the analysis presented in this section, it is possible to synthesize a response to its central question: Bitcoin, and especially Blockchain, present numerous possible applications, which represent the primary future for the technology created by Satoshi Nakamoto, however, it is not the future Nakamoto himself envisioned. Despite diverging from the creator's original expectations, the adoption of Bitcoin and Blockchain in institutional and hybrid forms is essential for these technologies to achieve greater relevance, both in the traditional financial system and in the other areas discussed. In sum, the future of Bitcoin and blockchain will likely diverge from Nakamoto's original vision, evolving instead into hybrid systems shaped by institutional constraints and economic realities.

5: CONCLUSION

In conclusion, Bitcoin and blockchain technology appear to have a positive impact on economic growth in certain economies that have adopted cryptocurrencies, such as different Asian countries and Bhutan. However, this impact remains relatively limited, and structural constraints such as the high cost of security prevent these systems from playing a larger role in major national economies.

Looking forward, the most promising future for these technologies may lie in their integration with the traditional financial system. Bitcoin itself may increasingly be traded through regulated financial products, as institutions such as BlackRock have already begun to offer.

Meanwhile, many economists believe that blockchain technology may have broader long term potential than Bitcoin itself. Blockchain could be implemented beyond the cryptocurrency ecosystem, including in public administration, where governments and municipalities have already begun experimenting with blockchain based systems.

In addition, blockchain technology could potentially be incorporated into global financial infrastructure such as the SWIFT network, particularly through permissioned blockchain systems. These systems could provide greater security than public blockchains like the Bitcoin network while offering advantages such as increased transaction speed, improved efficiency, lower operational costs, and continuous operation. Finally, based on the conclusions drawn regarding the future of Bitcoin and blockchain within the traditional financial system, an important question emerges, particularly when considering the potential impact of blockchain adoption in the SWIFT system: Are we experiencing a paradigm shift in the financial transaction system as we know it?

REFERENCES

S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” in Proc. IEEE, 2015.

J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE, vol. 15, no. 3, pp. 2084 - 2123, 2017.

K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

V. Gramoli, “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication,” in Proc. IEEE Int. Conf. Distributed Computing Systems Workshops, 2017.

M. Swan, “Blockchain: Blueprint for a New Economy. Sebastopol” CA: O’Reilly Media, 2015.

K. Croman et al., "Rethinking Permissioned Blockchains," in Proc. IEEE Int. Conf. Distributed Computing Systems, 2016.

J. Bonneau et al., "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in Proc. IEEE Symp. Security and Privacy, pp. 104–121, 2015.

G. Kiayias, A. Russell, B. David, and R. Oliynykov, "The Bitcoin Backbone Protocol: Analysis and Applications," in Advances in Cryptology (EUROCRYPT), pp. 281–310, 2015.

Z. Mourad and M. Gül, "Crypto-Driven Growth: A Comparative Study of Bitcoin and Ethereum on Economic Growth for Multi-Country Analysis," Russian Journal of Economics, vol. 11, no. 4, pp. 403–425, 2025.

P. B. Titalessy and R. J. Situmeang, "Bitcoin on Economic Growth (Case of 8 Asia Countries)," International Journal of Accounting & Finance in Asia Pacific, vol. 7, no. 1, pp. 110–123, 2024.

G. O. T. Utomo, "The Influences of Cryptocurrency on Economic Growth: Case Study of Bitcoin in Five Asian Countries (2011–2016)," Universitas Brawijaya, Indonesia, 2018.

M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on the Security of Blockchain Systems," Future Generation Computer Systems, vol. 107, pp. 841–853, 2020.

M. Casino, T. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," Telematics and Informatics, vol. 36, pp. 55–81, 2019.

A. Gervais et al., "On the Security and Performance of Proof-of-Work Blockchains," in Proc. ACM Conf. Computer and Communications Security, pp. 3–16, 2016.

X. Xu et al., "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities," IEEE Access, vol. 7, pp. 117134–117151, 2019.

C. D. Krause and T. Tolaymat, "Quantification of Energy and Carbon Costs for Mining Cryptocurrencies," Joule, vol. 2, no. 11, pp. 2368–2378, 2018.

I. Eyal and E. G. Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," in Financial Cryptography and Data Security, pp. 436–454, 2014.

J. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–238, 2015.

M. Javarone and M. Wright, "From Bitcoin to Bitcoin Cash: A Network Analysis," in Proc. Advances in Social Networks Analysis and Mining, 2018.

C. Catalini and J. S. Gans, “Some Simple Economics of the Blockchain,” NBER Working Paper No. 22952, 2016.

L. W. Cong and Z. He, “Blockchain Disruption and Smart Contracts,” NBER Working Paper No. 24399, Mar. 2018.

I. Makarov and A. Schoar, “Blockchain Analysis of the Bitcoin Market,” NBER Working Paper No. 29396, 2021.

J. Ma, J. Gans and R. Tourky, “Market Structure in Bitcoin Mining,” NBER Working Paper No. 29396, 2021.

B. Bollinger and E. Mansur, “When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy,” NBER Working Paper No. 31312, 2023.

D. Yermack, “The Potential of Digital Currency and Blockchains,” NBER Reporter, 2018.

J. S. Gans and H. Halaburda, “‘Zero Cost’ Majority Attacks on Permissionless Blockchains,” NBER Working Paper No. 31473, 2023.

J. S. Gans, “The Fine Print in Smart Contracts,” NBER Working Paper No. 25443, 2019.

D. Cai, Y. Qian and N. Nan, “Blockchain for Timely Transfer of Intellectual Property,” NBER Working Paper No. 30913.

M. Bordo and W. Roberds, “Central Bank Digital Currencies: An Old Tale with a New Chapter,” NBER Working Paper No. 30709.

E. Budish, “Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains,” Quarterly Journal of Economics, vol. 140, no. 1, pp. 1–62, 2025.

G. Msefula, T. C. Hou, and T. Lemesi, "Financial and Market Risks of Bitcoin Adoption as Legal Tender: Evidence from El Salvador," *Humanities and Social Sciences Communications*, vol. 11, article no. 1396, 2024.

J. Almeida and T. C. Gonçalves, "A Decade of Cryptocurrency Investment Literature: A Cluster-Based Systematic Analysis," *International Journal of Financial Studies*, vol. 11, no. 2, article 71, May 2023.

P. Kayal and P. Rohilla, "Bitcoin in the Economics and Finance Literature: A Survey," *SN Business & Economics*, vol. 1, no. 7, 2021.

S. López-Sorribes, J. Rius-Torrentó, and F. Solsona-Tehàs, "A Bibliometric Review of the Evolution of Blockchain Technologies," *Sensors*, vol. 23, no. 6, article 3167, Mar. 2023.

M. Xu, X. Chen, and G. Kou, "A Systematic Review of Blockchain," *Financial Innovation*, vol. 5, no. 1, pp. 1–14, 2019.

K. Wnęk, "El Salvador's Adoption of Bitcoin from the Perspective of One Year: The Influence on the State Budget and a Comparison to Poland's Legislature," *Krakow University of Economics / Malopolska School of Public Administration*, 2022.

M. Dutra, A. Tumasjan, and I. Welpe, "Blockchain Technology as a Driver of Economic Development in Small Economies: A Dynamic Capabilities Framework," *Journal of Small Business Management* (Taylor & Francis), vol. 62, pp. 413–438, 2023.

M. Á. López-Cabarcos et al., "Decentralized Finance in Business and Economics Research: A Bibliometric Analysis," *International Journal of Financial Studies*, vol. 13, no. 4, article 211, 2025.

D. Levis, F. Fontana, and E. Ughetto, "A Look into the Future of Blockchain Technology," *PLOS ONE*, vol. 16, no. 11, article e0258995, Nov. 2021.

A. Capponi, R. Jia, and K. Y. Wang "Maximal Extractable Value and Allocative Inefficiencies in Public Blockchains," Journal of Financial Economics, vol. 172, article 104132, 2025.

M. Niforos, "Blockchain in Financial Services in Emerging Markets, Part II: Selected Regional Developments," World Bank, 2017.

T. Adrian et al., "Understanding Stablecoins," IMF Departmental Paper No. 2025/009, International Monetary Fund, December 2025.

B. Adhikari, "Bitcoin and Digital Currency Mining in Bhutan," Bhutan Watch, 2026.

M. Gul, S. Hashim, and A. Hayat, "The Impact of Macroeconomic Indicators on Bitcoin: A Case Study on Pakistan," *Journal of Social Research Development*, vol. 4, no. 2, pp. 400–409, June 2023.

O. A. Ogunode, A. T. Iwala, O. A. Awoniyi, B. O. Amusa, T. R. Omosebi, S. K. Kassim, and R. I. Akintoye, "Cryptocurrency and Global Practices: Lessons for Nigeria," *South Asian Journal of Social Studies and Economics*, vol. 15, no. 1, pp. 7–28, 2022.

A. T. Mazikana, "The Impact of Cryptocurrencies in Zimbabwe: An Analysis of Bitcoins," SSRN Working Paper, 2018.

P. Pumcharoen, "The Impact of Bitcoin Adoption on Economic Growth: An Empirical Case Study of El Salvador," Master's Thesis, Charles University, Prague, July 2024. Supervisor: prof. PhDr. Ladislav Krištoufek, Ph.D.

N. Kiyotaki and R. Wright, " A Contribution to the Pure Theory of Money" Journal of Economic Theory, Vol. 53 No. 2, pp. 215-235, 1991

S. Singh et al., "What We Know and What Should We Know About the Future of Blockchain in Finance," *PMC / Open Access*, 2024.

M. Kassen, "Blockchain and Public Sector Innovations: Understanding Decentralized Models of Technology Adoption in E-government," *Innovation: The European Journal of Social Science Research*, 2025.

Y. Hong et al, ""The Impact of Bitcoin ETF Approval on Bitcoin's Hedging Properties Against Traditional Assets" arXiv Working Paper, December 2025.
Bayram, Talay and Kutlu, "SWIFT vs. Blockchain," *Information Systems Research*, 2024. 29