**Why do Banks Oppose Digital Currency**

**Shivani Chauhan** – 22GSOB2010073

**Under the Guidance of**

**Prof. Ranjul Rastogi**

**GALGOTIAS UNIVERSITY**

**ABSTRACT**

In response to the declining use of cash and increased competition from Big Tech companies, cryptocurrencies, and stablecoins, many central banks in advanced economies are considering issuing central bank digital currencies . One critical aspect of Digital currency design is transaction privacy. Existing solutions often face security concerns or fail to provide complete privacy similar to cash transactions. Additionally, there's a concern that fully private payment systems may not comply with anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations. This paper adopts a design science research approach (DSR) to develop and assess a comprehensive software-based Digital currency system that facilitates fully private transactions while adhering to regulatory constraints. Using zero-knowledge proofs (ZKPs), the system enforces privacy limits on transactions without revealing transaction details to third parties. Interviews with economic, legal, and technical experts confirm the feasibility of a regulatorily compliant Digital currency system based on ZKPs, supporting full privacy similar to cash transactions.

**INTRODUCTION**

Banks' opposition to digital currencies is rooted in a complex web of concerns, ranging from regulatory uncertainties to competitive pressures and technological challenges. At the core of this opposition lies a fundamental fear of losing control. Banks have historically held a dominant position in the financial system, wielding significant power over currency issuance, transaction processing, and financial intermediation. The advent of digital currencies threatens to disrupt this established order by introducing decentralized systems that operate outside traditional banking channels.

One major concern for banks is the regulatory ambiguity surrounding digital currencies. Unlike traditional financial instruments, digital currencies often operate in a regulatory gray area, with rules and guidelines that vary widely across jurisdictions. Banks, bound by strict anti-money laundering (AML) and know-your-customer (KYC) regulations, are wary of the compliance risks associated with digital assets. The lack of clear regulatory frameworks for digital currencies can leave banks vulnerable to legal and reputational risks, discouraging them from fully embracing these emerging technologies.

Moreover, digital currencies pose a significant competitive threat to banks' traditional business models. Decentralized cryptocurrencies like Bitcoin offer lower transaction fees, faster settlement times, and greater accessibility compared to traditional banking services. This can potentially lure customers away from banks, eroding their market share and profitability. Banks also face pressure from fintech startups and non-bank entities that are leveraging blockchain technology to offer innovative financial products and services, further intensifying competition in the industry.

The inherent volatility and risk associated with digital currencies also give banks pause. Many cryptocurrencies experience extreme price fluctuations, making them unsuitable for traditional banking activities such as lending and investment. Banks are wary of the speculative nature of digital assets and the potential for significant losses. Additionally, security concerns, including hacking, theft, and fraud, pose significant challenges for banks looking to integrate digital currencies into their systems. The decentralized nature of cryptocurrencies makes them attractive targets for cyberattacks, raising questions about the security and integrity of these assets.

Furthermore, the emergence of central bank digital currencies (CBDCs) adds another layer of complexity to the equation. While some banks may see CBDCs as an opportunity to collaborate with central banks and streamline payment systems, others view them as a direct threat to their traditional business models. CBDCs could potentially disintermediate banks by allowing individuals and businesses to hold digital currency directly with the central bank, bypassing commercial banks altogether.

In addition to regulatory, competitive, and technological challenges, banks also grapple with legacy systems and infrastructure that may not be easily adaptable to accommodate digital currencies. Updating these systems to support the complexities of blockchain technology can be costly and time-consuming, deterring banks from fully embracing digital currencies.

In summary, banks' opposition to digital currencies stems from a combination of regulatory concerns, competitive pressures, technological challenges, and fears of losing control. While some banks may cautiously explore opportunities to leverage blockchain technology and collaborate with central banks in the development of CBDCs, many remain hesitant or even resistant to fully embracing the disruptive potential of digital currencies.

**LITERATURE REVIEW**

In another study focusing on organisations, **(Andrychowicz et al. 2016)** approach examining organisation perspectives by developing a protocol for analysing the possibility of using bitcoin for a secure lottery system. **(Andrychowicz et al.)**’s study explored the possibility of designing an online protocol for playing lottery in a decentralized way, therefore addressing possible lottery organisation protocol modelling.

A similar study focused on organisational modelling, **(Kazan et al. 2015)** examined organisations to understanding how CC companies create and capture the value of their digital business models, with consideration of the potentially disruptive capabilities associated with the technology. Contrary to the review by **(Morisse 2015)** where the author identified the lack of new business models based on DC, the investigations by **(Andrychowicz et al.)** and **(Kazan et al.),** provide evidence that research on DC continues to evolve by addressing the need for new business models.

The study by **(Van Alstyne 2014),** evaluate the nature of Digital Currency to prove that the system has value andshould be accepted as a currency and innovative payment system. (Van Alstyne) also, examines the evolving DC phenomenon with particular reference to the systems protocol.

**(Cusumano 2014)** and**(Glaser and Bezzenberger 2015**) address similar issues of providing a better understanding of DC.While the study by **(Cusumano 2014)** is focused on providing an evaluation of Digital Currency ecosystem.

**(Glaser and Bezzenberger 2015)** Focuses on classifying various Decentralized Consensus Systems based on their characteristics. In the study by (Meiklejohn et al. 2016), the author also examines the characteristics of DC. Meiklejohn investigated the characterization of Digital Currency network with a particular aim of understanding the possible anonymity in the protocol design and the actual anonymity of its users.

**OBJECTIVE**

**Objectives of Digital currency**

Digital currency, like any other form of currency, serves several objectives:

**Efficiency:** Digital currency aims to streamline transactions, making them faster and more convenient. With digital currency, transactions can occur instantaneously, reducing the need for intermediaries like banks and clearinghouses.

**Accessibility:** Digital currencies can be accessed by anyone with an internet connection, providing financial services to people who may not have access to traditional banking systems.

**Security:** Blockchain technology, which underlies many digital currencies like Bitcoin, provides a high level of security through cryptographic techniques. Transactions are tamper-proof and transparent, enhancing trust among users.

**Lower Costs:** Digital currencies can potentially reduce transaction fees associated with traditional banking systems, especially for international transactions, where fees and exchange rates can be significant.

**Financial Inclusion**: By bypassing traditional banking systems, digital currencies can empower individuals in underserved or unbanked populations to participate in the global economy.

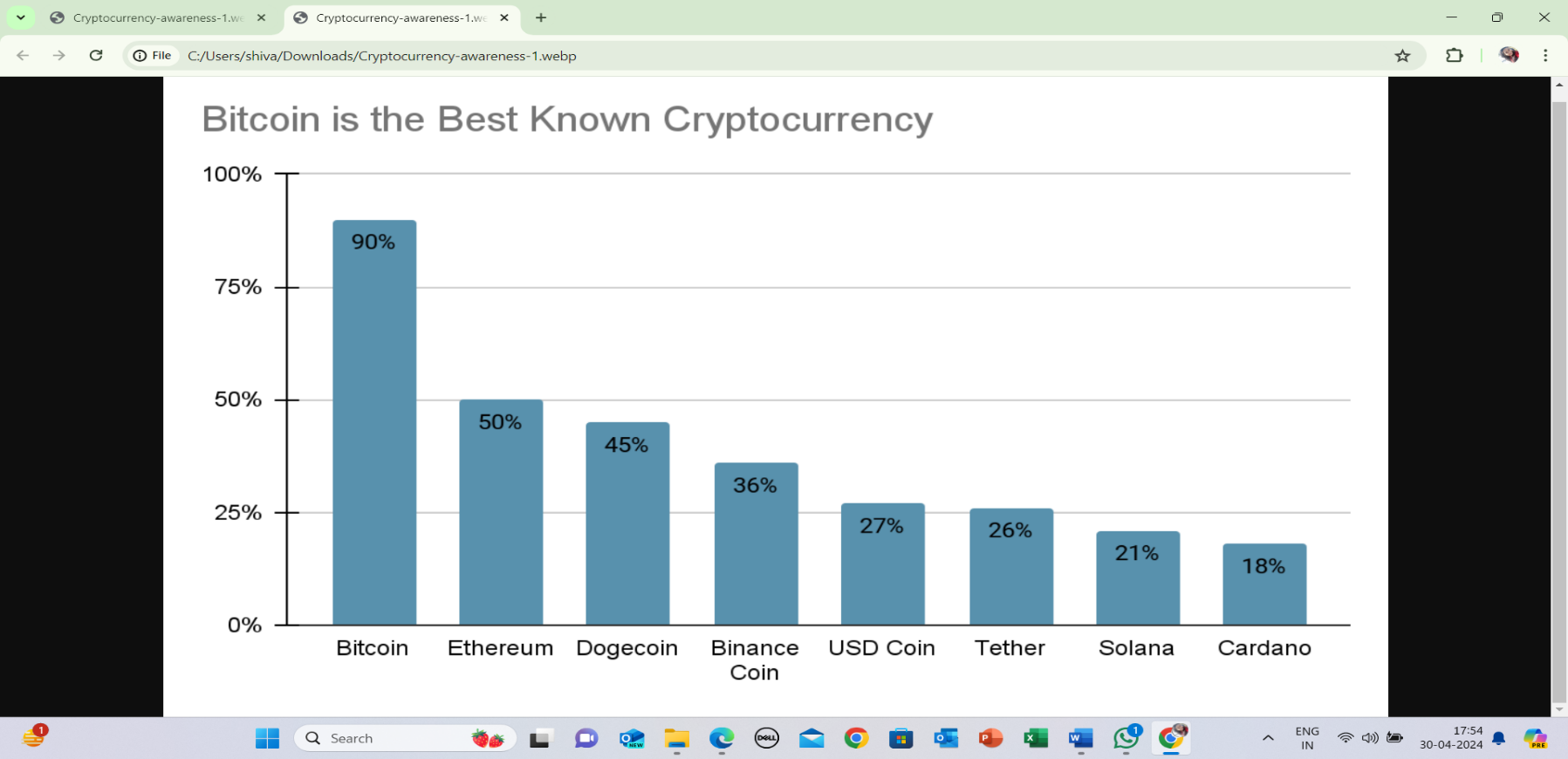
**Privacy:** While digital currencies offer transparency through the blockchain, they also offer varying degrees of privacy. Users can control the amount of personal information they share during transactions.

**Decentralization:** Many digital currencies operate on decentralized networks, meaning they are not controlled by any single entity or government. This decentralization can prevent manipulation and censorship of the currency.

**Innovation**: Digital currencies open up avenues for innovation in financial technology (fintech), including smart contracts, decentralized finance (DeFi), and new forms of asset tokenization.

Overall, the objectives of digital currency revolve around creating a more efficient, accessible, secure, and inclusive financial system.

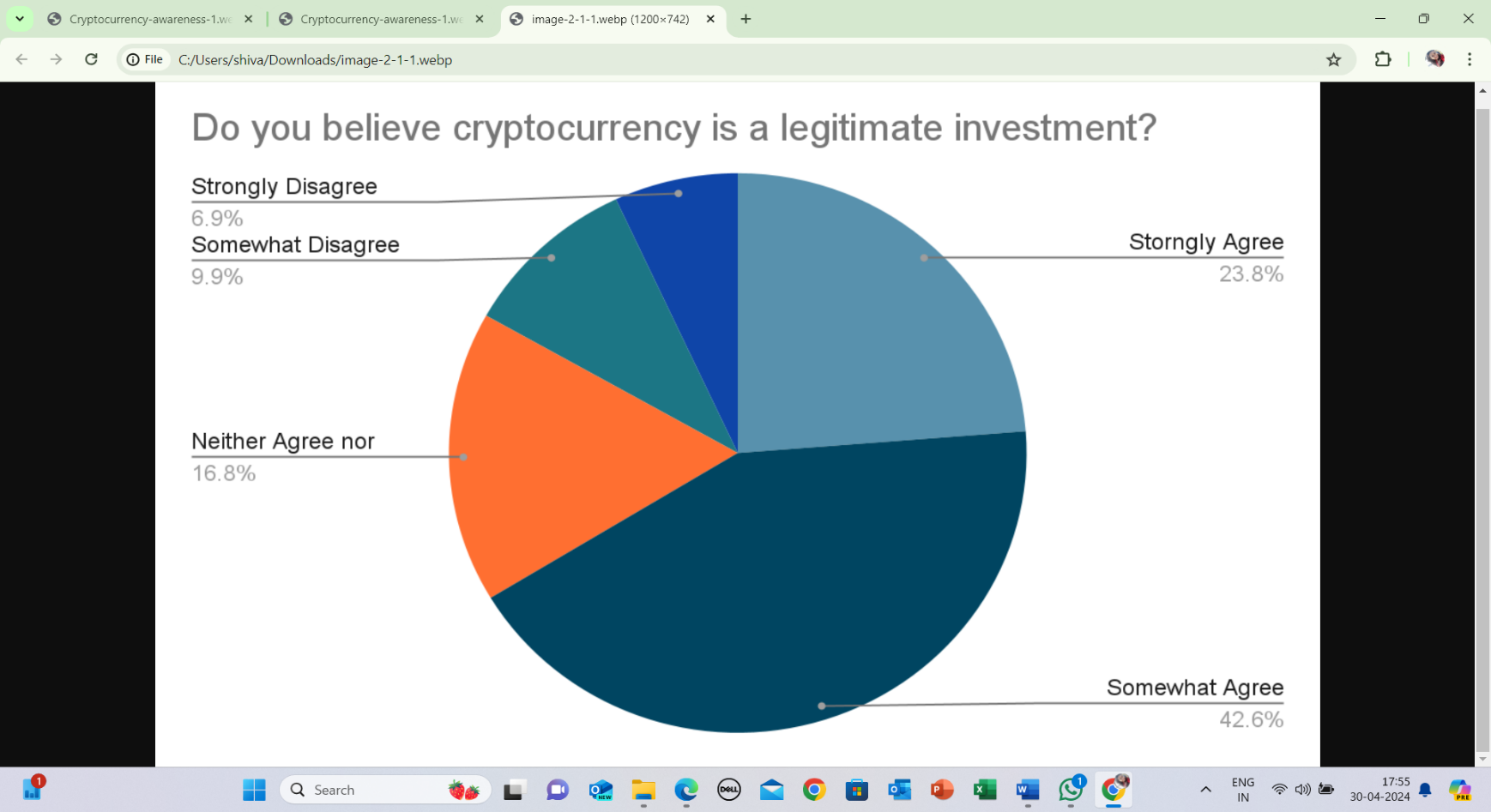
**DATA ANALYSIS**



**Legitimacy of Cryptocurrency: -**

According to the survey: -

* Almost 67% agree that cryptocurrency is a legitimate form of investment (either strongly or somewhat agreeing with this statement).
* Almost 17% neither agree nor disagree with that statement.
* Almost 17% disagree that cryptocurrency is a legitimate investment.



Meanwhile, 24% of those who invest in cryptocurrency say they trust it more than traditional investments, while, according to the FCA in the UK, some 60% of crypto holders said that they were happy to trade in the cryptocurrency market despite it being unregulated.

**Source: -** <https://www.forbes.com/advisor/au/investing/cryptocurrency/cryptocurrency-statistics/>

**FINDINGS**

**Opposing Digital Currency by the Government**

Opposition from governments against individuals exploiting digital currencies for money laundering is a significant concern. Governments worldwide are increasingly recognizing the potential risks associated with digital currencies, including their potential use for illegal activities such as money laundering and terrorist financing.

To address these concerns, governments have been implementing regulations and enforcement measures aimed at combating money laundering in the digital currency space. These measures often include:

KYC/AML Regulations: Governments impose Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations on digital currency exchanges and other service providers. These regulations require platforms to verify the identities of their users and report suspicious transactions to authorities.

Licensing and Registration: Some governments require digital currency exchanges and other businesses operating in the crypto space to obtain licenses or register with regulatory authorities. This helps ensure that these businesses comply with regulatory standards and can be held accountable for facilitating illicit activities.

Monitoring and Enforcement: Regulatory agencies monitor digital currency transactions and investigate suspicious activities. They may collaborate with law enforcement agencies to track down individuals involved in money laundering or other illegal activities using digital currencies.

Public Awareness and Education: Governments also invest in public awareness campaigns and educational initiatives to inform individuals about the risks associated with digital currencies and the consequences of engaging in illegal activities.

Overall, while digital currencies offer many benefits, including increased financial inclusion and innovation, it's crucial to address the risks of misuse, particularly for money laundering. Governments play a vital role in implementing regulations and enforcement measures to prevent illicit activities in the digital currency space and protect the integrity of the financial system.

**Opposing Digital Currency by the Banks**

Banks have also been increasingly vigilant in their efforts to combat money laundering facilitated by digital currencies. Here are some ways in which banks oppose individuals taking advantage of digital currencies for money laundering:

Transaction Monitoring: Banks employ sophisticated monitoring systems to detect suspicious transactions, including those involving digital currencies. They use algorithms and machine learning techniques to analyze transaction patterns and identify potentially illicit activities.

Enhanced Due Diligence: Banks apply enhanced due diligence measures when dealing with customers or businesses involved in digital currency transactions. This may include additional verification procedures and closer scrutiny of the source of funds.

Blocking or Suspending Transactions: Banks may block or suspend transactions involving digital currencies if they suspect money laundering or other illegal activities. They have the authority to refuse service to customers engaged in suspicious behavior.

Collaboration with Regulatory Authorities: Banks collaborate with regulatory authorities to share information and report suspicious activities related to digital currency transactions. This collaboration helps strengthen the overall efforts to combat money laundering in the financial system.

Customer Education: Banks also play a role in educating their customers about the risks associated with digital currencies and the importance of complying with anti-money laundering regulations. This may include providing information on the potential legal and financial consequences of engaging in illicit activities.

By taking these measures, banks aim to protect the integrity of the financial system and prevent the misuse of digital currencies for money laundering purposes. However, it's also essential for banks to strike balance between preventing illicit activities and fostering innovation in the digital currency space.

**CONCLUSION**

In conclusion, banks often oppose digital currency due to a combination of factors that challenge their traditional role, regulatory uncertainties, competitive threats, risk concerns, and technological challenges. The emergence of digital currencies, particularly decentralized ones like Bitcoin, fundamentally alters the dynamics of financial transactions by bypassing traditional banking intermediaries. This disruption poses a direct threat to banks' revenue streams and their established business models. Moreover, the regulatory ambiguity surrounding digital currencies creates compliance challenges and legal risks that banks are hesitant to navigate. Additionally, the potential competition posed by digital currencies, offering faster and cheaper payment solutions, threatens banks' market share and profitability. Concerns about the volatility of digital currencies, coupled with their association with illicit activities, further deter banks from embracing them. Lastly, integrating digital currencies into existing banking infrastructure requires substantial investment in technology and security measures, posing significant operational challenges. As a result, while some banks may explore opportunities in the digital currency space, many remain cautious and resistant to its adoption.

**REFERENCES**

<https://www.boj.or.jp/en/announcements/>

<https://www.boj.or.jp/en/announcements/>

<https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf>

<https://pic.bankofchina.com/bocappd/report/201704/>

<https://www.boi.org.il/en/NewsAndPublications/PressReleases/Documents/>

<https://www.lb.lt/en/news/>

<https://news.bitcoin.com/central-banks-testing-digital-currencies/>

<https://halshs.archives-ouvertes.fr/halshs-00414496>

<https://www.bis.org/publ/bppdf/bispap107.pdf>

<http://www.nber.org/papers/w23711>

<https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm>

<https://www.federalreserve.gov/newsevents/speech/files/brainard20190805a.pdf>

<https://www.bceao>.

<https://news.bitcoin.com/central-banks-testing-digital-currencies/>

<https://halshs.archives-ouvertes.fr/halshs-00414496/>

<https://www.bis.org/publ/bppdf/bispap107.pdf>

<http://www.nber.org/papers/w23711>

<https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm>

<https://www.federalreserve.gov/newsevents/speech/files/brainard20190805a.pdf>