

Report on the Applicability of Virtual Currency

Posted on February 16, 2024

Introduction

As a result of recent technological advancements and an increased emphasis on collecting the latest information, online sources have emerged as the most reliable information resources. Today, most people rely on internet-based transportation and communication systems, including traffic signal control and flight navigation, electronic mail, text messaging, and mobile phones. The worrying increase in vulnerabilities and risks in digital systems is a direct result of our reliance on the internet. If these threats materialized, it would hurt the company. The risk of cybercriminals breaking into cryptocurrency exchanges and stealing customer funds is high because of the nature of dealing with [virtual currency](#). As the chief information security officer (CISO), I am responsible for ensuring that the virtual currency has a very high level of cybersecurity to guarantee the clients' accountability, transparency, and safety.

Application of Virtual Currency to Financial Services

The widespread use of virtual currencies is anticipated to have far-reaching effects on the global economy because of the security and anonymity they provide for monetary transactions. Virtual currency allows consumers to make purchases without carrying large quantities of cash. Companies such as Rakuten and PayPal are examples of those that have embraced the digital currency system (Pazarbasioglu et al.,2020). Although it has its drawbacks, virtual currency still has no equal when efficiently managing transactions. On top of that, virtual currency is more cost-effective than traditional ways of payment. It has lower transaction fees than Western Union and PayPal, for starters. Customers, mindful of the economy's current situation, are constantly looking for methods to save costs. The low transaction costs of virtual currency allow businesses to keep their data and information safe while staying ahead of the competition.

The steady development of new technologies has allowed digital currency to carve out a specialized market in the banking industry. Sweden and Ecuador are just two countries that have switched to using electronic currency as a direct result of the rise of virtual currencies. Central banks in these countries use virtual money to make it easier for their customers to transact with them (Pazarbasioglu et al.,2020). Experts predict that in the not-too-distant future, virtual currencies will be as ubiquitous as credit cards. Digital currency can be utilized both at home and abroad. Users can now use Bitcoin

as a means of payment when purchasing things from abroad. Transactions are speedy, secure, and less cumbersome than those processed by traditional payment systems.

Encryption Technology Without Virtual Currency

Bitcoin's crucial blockchains are encrypted using public-key technology to prevent theft. Bitcoin mining rigs can use this encryption approach without problems; however, they still need trustworthy and up-to-date security software and public keys (Zhang& Huang,2022). Public-key cryptography is the foundation of cryptocurrency value since it ensures that transactions are private and untraceable, even if a computer is used to make the payment. When the internal network is designed, customers' and workers' personal information (PII) should be encrypted using the latest encryption technology (Zhang& Huang,2022). So, digital money used for trade and finance must be easily accessible on various platforms. There are both symmetric and asymmetric approaches to encrypting data. Asymmetric encryption, in contrast to symmetric encryption, does not rely on the ideas of substitution and permutation but rather on solving a difficult mathematical problem.

Recommendations

Employing encryption on your electronic devices is an excellent safeguard for your data. Encryption protects computer systems and data from internet dangers such as hacking and data loss. Virtual currency employs encryption technologies to protect user information and keep transactions private. It is feasible to discover how cryptography is utilized in digital currencies through private key cryptography. Using private keys to encrypt and decrypt data enables access to digital currency exchanges. Users risk permanent capital loss without private keys because they cannot access their data. In place of virtual currency, platforms for non-financial transactions may use encryption technologies. Encryption is crucial to developing virtual currencies because it enables secure and straightforward transactions and protects customers. Asymmetric encryption, which employs both [blockchain technology](#) and private keys, is essential for enhancing the security of bitcoin transactions. Certainly, this is the strongest argument.

Customers may be able to make quicker and more informed decisions about what they buy as a result. While transacting with a virtual currency, there are no restrictions that could be a hassle for clients. But companies should accept digital currency as electronic cash so that customers can pay with it (Naheem,2018). Information about customers will be protected during transactions. For smooth financial dealings, companies should make customer security a primary priority. As a result, using a digital currency will provide customers with a safe channel for transacting business with the company (Naheem,2018). Nonetheless, clients should be vary owing to security threats like phishing, fraud, and hackers. They can be prevented by using best practices for data hygiene and security measures like firewalls to protect against malware.

The cost-benefit analysis should be taken into account as well. Virtual currency users incur minimal costs while enjoying massive advantages. Bitcoin purchases, for instance, can be mutually beneficial. Bitcoin investors typically do not part with a significant chunk of change. The advantages of Bitcoin outweigh the potential costs associated with paying blockchain fees. Users can also benefit from safer financial dealings at reduced prices (Guesmi et al.,2019). As a bonus, users of virtual currencies don't have to worry about transaction costs because they are not taxed. Hence, the advantages of virtual currency outweigh the costs incurred by users. Since blockchain technology is necessary for Bitcoin, encryption technologies would be used to build support for the technology at little cost to the administration. Given the current worth of bitcoin and how its value has increased over time, it seems like a financially stable time to invest in the financial sector.

Using digital currency is simpler, quicker, and less expensive than traditional currencies. Due to several problems, such as payment recipient credentials, currency instability, regulatory agreements, and exchange risks, financial institutions are less enthused about virtual money than previously. One of the implications of digital money on financial organizations is increased proficiency. Financial companies will prosper because digital money makes payments simpler, faster, and more secure (Mazanec,2021). Without a doubt, using bitcoin by financial institutions has several benefits. If customer privacy is shielded from breaches and other incursions, client confidence in financial institutions will only rise. The company's reputation is growing as a result. Digital currency is utilized as a dependable and cost-effective replacement in unstable economies. Although the digital exchange is not extensively used, several nations do so because it gives their national currency financial protection against the unpredictability of fluctuating inflation rates. This seems to have the potential to replace money in the future.

Conclusion

Virtual currency will make future commercial interactions between businesses and customers more secure. Cloud computing, virtualization, and encryption benefit those using digital currency. Switzerland and Ecuador are two countries that have adopted Bitcoin for use in commercial transactions. Blockchain technology facilitates the use of digital currency. Users of digital currencies should exercise caution since cybersecurity vulnerabilities can lead to data breaches and identity theft. Those who use virtual currency are worried that crime will rise if the government doesn't take action. Users must keep their encryption keys safe to prevent irreversible financial losses. To prevent malware and hacking, utilize firewalls and intrusion detection systems. As a result, Bitcoin is a game-changer for the banking sector. Businesses that deal in virtual currency, and their consumers, need to protect their private encryption keys to prevent hacking, fraud, and ransomware.

References

Bolt, W., & Van Oordt, M. R. (2020). On the value of virtual currencies. *Journal of Money, Credit and*

Banking, 52(4), 835-862.

Guesmi, K., Saadi, S., Abid, I., & Ftiti, Z. (2019). Portfolio diversification with virtual currency: Evidence from bitcoin. *International Review of Financial Analysis*, 63, 431-437.

Naheem, M. A. (2018). Regulating virtual currencies-the challenges of applying fiat currency laws to digital technology services. *Journal of Financial Crime*.

Mazanec, J. (2021). Portfolio optimalization on digital currency market. *Journal of Risk and Financial Management*, 14(4), 160.

Zhang, T., & Huang, Z. (2022). Blockchain and central bank digital currency. *ICT Express*, 8(2), 264-270.

Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. *World Bank*, 54.

Zhang, Q. (2021, January). An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption. In *2021 2nd International Conference on Computing and Data Science (CDS)* (pp. 616-622). IEEE.