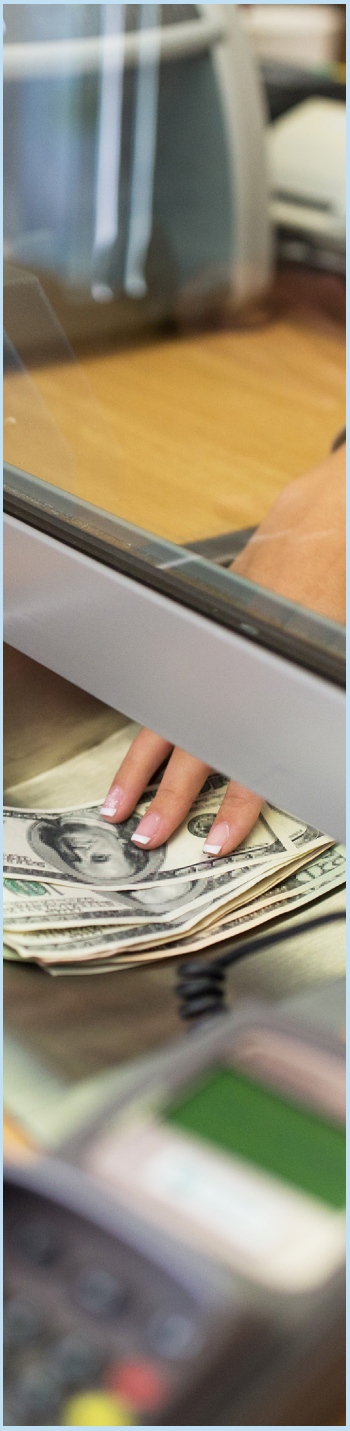
VIEW POINT



VALIDATION STRATEGIES FOR DIGITAL CURRENCY SYSTEMS

Abstract

Since their emergence some years ago, digital currencies are becoming increasingly mainstream. This is due to increased institutional adoption and the initiation of central bank digital currency (CBDC) projects by central banks and governments around the world. As they gain popularity, the technology empowering these digital currencies must evolve quickly to ensure security, stability, and scalability given the sensitive nature of digital currencies.

This paper examines why validation of the systems that support digital currencies is critical to their success. It also looks at possible strategies to comprehensively validate the technology imperatives of digital currency adoption at scale.

Infosys®
Navigate your next

Overview

Digital currency is an asset that is managed, stored, or exchanged on digital computer systems over the Internet and exists only in electronic format. There are several forms of digital currency such as cryptocurrency, central bank digital currency (CBDC), virtual currency, etc. The backbone of a digital currency system is blockchain, a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

The characteristics of two such digital currencies, i.e., cryptocurrency and CBDC that have gained traction in recent years are compared below.

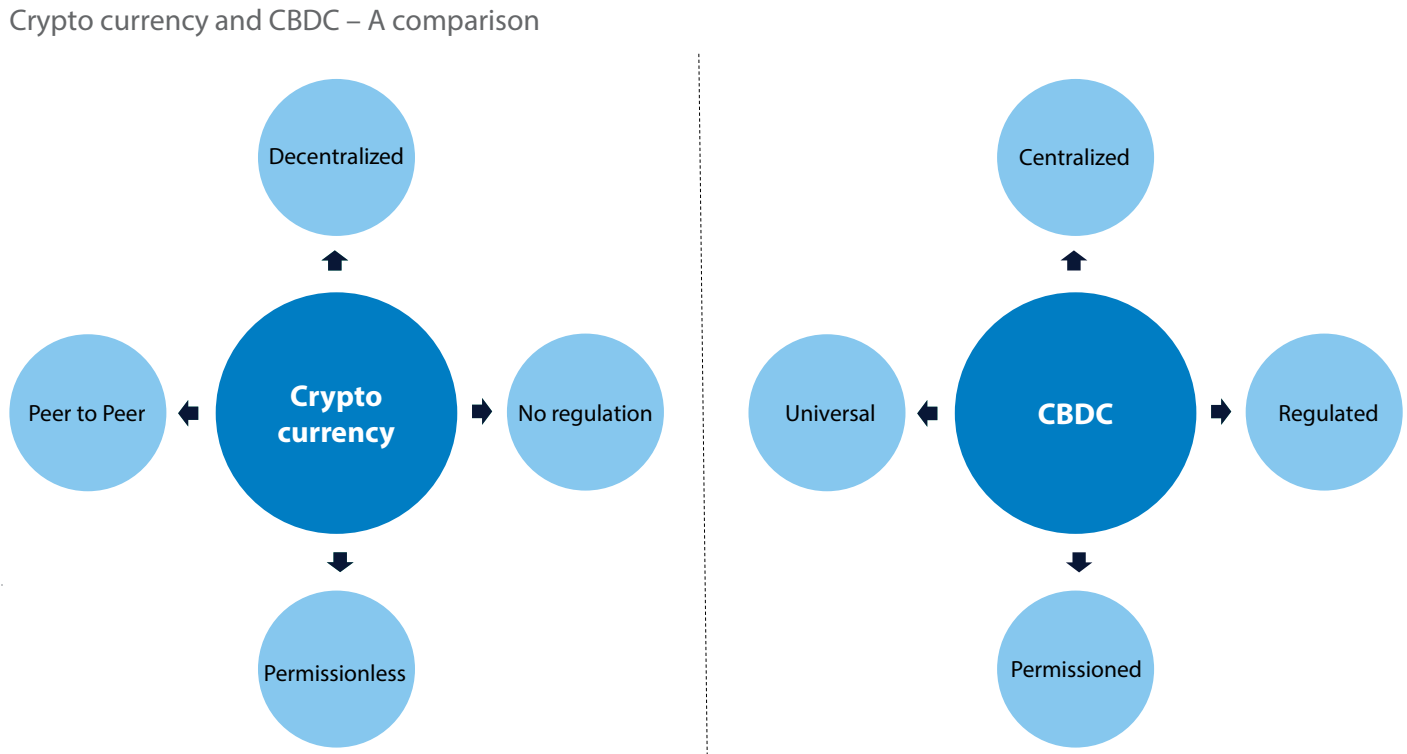


Figure 1 – Cryptocurrency and CBDC – A comparative view

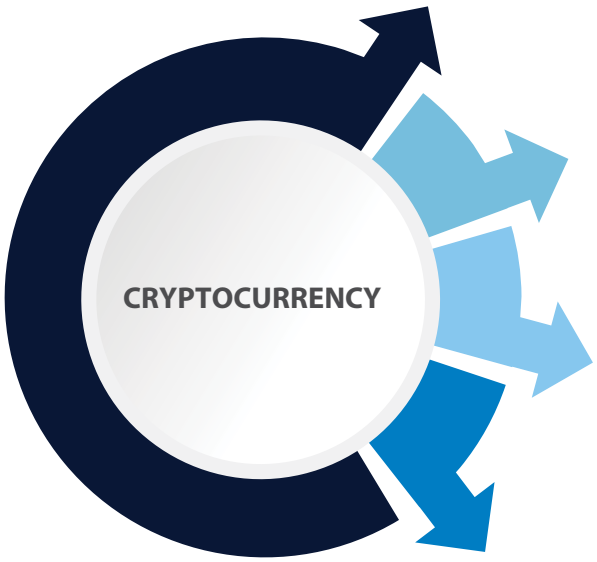
Cryptocurrency is a digital currency that is based on blockchain technology in which transactions are verified and records maintained by a decentralized system using cryptography. In 2009, Bitcoin, the first decentralized cryptocurrency was introduced. Today, there are over 10,000 active cryptocurrencies in existence.

Central bank digital currency (CBDC) is the digital equivalent of a fiat currency issued by a nation's central bank or monetary authority that may or may not be based on blockchain or distributed ledger. CBDCs can be applied in two areas:

- **Interbank/Wholesale** – The use of CBDCs is restricted to financial institutions for interbank payments, financial payment processes, cross-border payments by including multiple currencies and jurisdictions, etc. Use cases related to such transactions have to be tested keeping in mind central and affiliate banks.
- **Retail** – In the retail market, CBDCs are used by citizens of a country. It is incorporated as a digital form of cash to exchange money. The validation of use cases around money exchange is critical.

There are several forms of cryptocurrency and CBDCs as depicted in the picture below.

Forms of Cryptocurrency



Proof of Work (PoW)

A type of consensus algorithm where the computational effort expended is proven by a party, e.g., Bitcoin, Ethereum

Proof of Stake (PoS)

A consensus mechanism where validators are selected in accordance with their stake in a cryptocurrency, e.g., Eos, Tron

Tokens

Tokens are digital assets built on another cryptocurrency's blockchain, e.g., Utility coin, Security Coin etc.

Stable Coins

A type of crypto currency whose value is tied to another currency, commodity or financial instrument, e.g., Paxos, Gemini

Figure 2 – Forms of cryptocurrencies

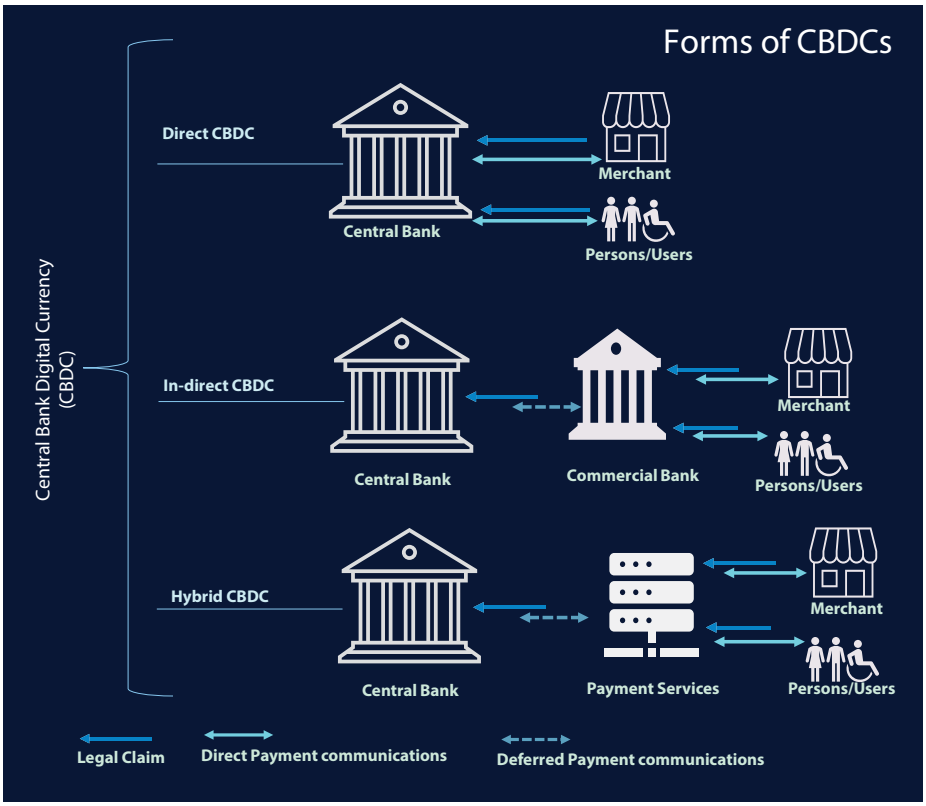


Figure 3 – Forms of CBDCs

Analysts estimate that the global cryptocurrency market will triple by 2030. The crypto market is likely to become more regulated and offer some stability and transparency. Over time, some cryptos may be valued higher while others cease to exist. Wider institutional adoption of cryptos is expected as companies across industries show interest in its applications and, in some cases, buy shares in the crypto market as well.

As governments across the globe look at adopting new financial technologies to solve a multitude of problems, CBDCs could feature in their priority list. As of today, 9 countries globally have launched CBDCs and nearly 87 countries are exploring the potential of CBDCs with trials in various stages.

All this points to a future where digital currencies could very well be an integral part of financial systems across the world.

Digital Currencies – The Future of Money

Digital currencies have evolved over time to become more acceptable in the global community. While cryptocurrencies were initially met with suspicion and hesitance, today they are one of the more popular investment avenues. Some studies suggest that there are over 6,000 types of cryptocurrencies in existence, the popular ones being Bitcoin, Ethereum, Dogecoin, and Litecoin. With increasing adoption and acceptance of cryptocurrencies, these can potentially find application in low-cost money transfers, medium of investment, and payments modes.

Governments and central banks across the world are working hard to make CBDCs a reality for several reasons. CBDCs have lower transaction costs and are, therefore, more cost efficient than physical cash. They promote financial inclusion by providing easier and safer access to money for unbanked populations and support quick and seamless monetary policy flow. CBDCs also help governments and central banks offer a healthy competition to private firms that need incentives to meet transparency standards.

Given the rising acceptance of cryptocurrency and its popularity in emerging markets, many industries are embracing digital coin transfers and constructing their business models around these. Some examples are the online gaming industry, hospitality sector, retail markets, and social platforms. On the other hand, there are those who do not subscribe to the idea of cryptocurrency or its legitimacy owing to challenges such as cybersecurity issues, scalability, and limited or lack of regulations.

On the CBDC front, a majority of developed and emerging markets are experimenting with the applicability of digital currencies for their economies. While many countries have initiated research, quite a few are running proofs of concept and pilots with their versions of CBDCs. In fact, more recently Nigeria became the first African country to launch its CBDC called e-naira.

In a nutshell, digital currencies are likely to find their way to mainstream use cases and disrupt traditional payment and cash flow processes. With both private enterprises and governments investing in this area, more and more people are likely to start using digital currencies sooner than later.

The Need for Validation

Digital currencies are primarily based on blockchain technology, the essence of which is decentralized control, high security, good scalability, stability and reliability, and immutability. Given the complexity, high stakes, and need for a robust fool-proof system, it is crucial to test and validate the software and systems powering digital currencies. While key aspects of traditional testing are applicable in the context of blockchain, there is a need for increased focus on non-functional aspects such as security, performance, network, and reliability considering the distributed architecture and technical complexities.

Newer realms of testing such as transaction testing, data transmission testing, testing the chain, block and node, etc., must be explored for the distributed network be it public, private, or permissioned. Performance and security testing are extremely important considering the high volume and criticality of transactions that could occur. In the context of CBDCs, in addition to the tests mentioned above, legal and compliance aspects may have to be validated given that these are highly regulated systems. Thus, validating digital currency systems may require higher technical competence as compared to traditional testing.

Some key considerations in testing digital currency systems are detailed below:

- **Functionality** – Testing of block and chain size, data transmission, and smart contracts are critical to ensure that the system operates seamlessly. API tests and integration tests ensure interconnected applications and systems work as expected.
- **Security** – Digital currencies usually have security built into their native design. Identity and access management involving multi-factor authentication and complex passwords are basic requirements. However, security is more important in the context of cryptocurrency exchanges, where fiat currencies are deposited to buy/trade cryptocurrency. The fact that crypto currency exchanges aren't backed by a central authority/ central bank and the holdings are not protected in the same way as traditional investments makes security testing imperative. Therefore, a 360-degree security test strategy is critical.
- **Resilience, reliability, and scalability** – Transactions in the digital currency world are time sensitive, critical, and can have high volumes. Hence, it is important to subject the system to extensive performance and reliability tests at the component as well as at the integrated system level.
- **Decentralized network** – Characterized by nodes, a decentralized set-up must be functionally tested for various activities such as transactions carried out at nodes, the integration between nodes, peer-to-peer testing, etc. Consensus mechanisms such as Proof of Work (PoW) /Proof of Stake (PoS) must also be validated.

All in all, when compared to traditional testing, the primary focus for digital currencies should be to test non-functional elements as well as features native to blockchain technology. While we understand the nuances of digital currency and the need for testing such systems, it is important to establish the right test strategies keeping in mind the various layers, interaction points, and components of blockchain.

Testing Imperatives for Digital Currencies

The table below highlights the key testing imperatives of digital currency both from a functional and non-functional standpoint.

Functional testing	Non-functional testing
Transaction testing Validation of transactions generated by the source application by considering authentication, authorization, completeness, and correctness	**Node testing** Nodes in a distributed network play a key role in mining/PoW and must be tested for functional, security, and performance aspects
API testing Testing the APIs on which the blockchain application depends for business capabilities	**Network testing** The decentralized nature warrants testing the underlying distributed network for performance and security
Integration testing Testing the interaction between components of Distributed Applications (DApps). Various integration points must be identified and tested for both success and failure scenarios	**Performance testing** Optimizing the time taken to execute transactions, smart contracts, chain size, block size, APIs, and integrations. It is important to test the transactions' broadcast time on network, time taken by a node to complete PoW, and the broadcast to other nodes by adding new blocks on the chain
Smart contract testing Validating the business rules/constraints governing smart contracts	**Security testing** Given the sensitive and trust-based nature of cryptocurrency and blockchain in general, validating security aspects at various failure points is vital. The top 10 security standards of the Open Web Application Security Project (OWASP) are a good reference point when designing security test scenarios
End-to-end user workflow testing Testing the business requirements of the blockchain application and user experience	**Resilience testing** It is important for a digital currency system to withstand various load conditions given the criticality of transactions. The network and nodes must be tested under various stress conditions and the response observed. Chaos testing methods and tools will help test the resilience of the system

Tools for Blockchain Testing

While test strategies are put in place, it is also important to identify the right tool set. Here, we have examined a few prominent tools available for blockchain testing.

Testing Tool	Description
Ethereum Tester	Open-source tool for testing Ethereum blockchain applications
Populus	A testing framework developed in Python and powered by pytest. It helps test smart contracts
Manticore	Manticore can analyze Ethereum smart contracts, Linux ELF binaries and WSM modules
Embark	Embark is used to deploy smart contracts on Ethereum Virtual Machine (EVM). It handles contract migration for multiple contracts and auto redeploys contracts if needed
Truffle	Truffle simplifies implementation of decentralized applications for engineers by providing a development environment, testing framework, and asset pipeline for building a blockchain application on Ethereum
Ganache	Ganache is a personal Ethereum blockchain used to test smart contracts where users can deploy contracts, develop applications, run tests, and perform other tasks at no cost. It is a part of the Truffle suite and is available in 2 forms i.e. UI and CLI
Exonum Testkit	This tool enables testing services and transactions across blockchain applications. In case of network testing, it helps auditing and validations
Corda Testing Tools	Corda is an open-source distributed ledger platform that comes with an in-built testing tool. It can help with writing test contracts and test smart contracts from functional, integration, and load testing's standpoint
Hyperledger Fabric Tool	Fabric tests provide two tools for testing the fabric itself, i.e., the operator tool and Performance Traffic Engine (PTE)

In addition to the above, tools for API testing, performance testing, and security testing, must also be evaluated.

Conclusion

Digital currencies are emerging as a long-term trend and are likely to attract greater focus in the future as a key medium of currency exchange. These could potentially be used alongside fiat currencies. As the supporting technology evolves and becomes more complex, comprehensive validation strategies will be needed to ensure better security, scalability, and stability. Security, performance testing, and other non-functional tests are of paramount importance and may take precedence over traditional testing needs in this scenario. It is, therefore, important to ensure that a best-in-class, all-encompassing test strategy is put in place to ensure a stable, secure, and robust digital currency system.

About the Authors

Gnanaben Vishalbhai Upadhyay
Technology Architect

Gnana has experience of over 13 years in the software industry and currently architecting key technical initiatives for a large financial service customer at Infosys

Harsha S.
Senior Project Manager

Harsha has experience of over 15 years in the software testing space and currently focuses on driving innovation, IP commercialization & deployment in the validation services unit at Infosys

References

1. Taxonomy of money, based on "Central bank cryptocurrencies" by Morten Linnemann Bech and Rodney Garratt.
2. https://www.researchgate.net/figure/The-money-flower-a-taxonomy-of-money-source-43-51_fig1_352790837
3. https://www.financemagnates.com/thought-leadership/industries-that-are-using-cryptocurrency/
4. https://www.atlanticcouncil.org/cbdctracker/
5. https://wirexapp.com/blog/post/the-8-different-types-of-crypto-assets-0471
6. https://www.icba.org/newsroom/blogs/main-street-matters/2021/06/03/digital-dollar-digest-what-central-bank-digital-currency-architecture-means-for-community-banks
7. https://www.impactqa.com/blog/5-topmost-tools-for-blockchainapp-testing/
8. https://blog.logrocket.com/complete-guide-blockchain-testing/
9. https://www.scnsoft.com/software-testing/tools-for-testing-blockchain-applications
10. https://www.bis.org/publ/qtrpdf/r_qt1709f.htm
11. https://cbdctracker.org/
12. https://learn.g2.com/types-of-cryptocurrency

For more information, contact askus@infosys.com

Infosys®
Navigate your next