DXC.technology

White Paper

The rising power of cryptoassets

What they are, what they can do for financial services organizations and how to design them

In 2009, bitcoin was the only cryptoasset on the market. Since then, bitcoin and its core blockchain technology have led to the birth of numerous other blockchains, each with its own cryptoassets. It's estimated that there are more than 2,000[1] cryptoassets today, with many more being created each month. These cryptoassets — new native digital assets such as cryptocurrencies or tokenized traditional assets such as real estate and gold — became a new asset class of resources with economic value owned or controlled by individuals, organizations or countries.

So, what exactly are cryptoassets, and where does their value come from? What opportunities do they bring to our economy and to organizations? And how do we best design them? In this paper, we demystify the complexity of cryptoasset design and point to ways financial services companies can leverage them to their advantage.

As an asset class, cryptoassets are equipped to play an important role in today's economies by revolutionizing the way we do business. They open doors for new business models and improve asset management — reducing friction and overhead costs, increasing liquidity, codifying rules and regulations, and increasing transparency throughout an asset's life cycle.

Technically, a cryptoasset is a digital representation of value or contractual rights — usually called a token — that is cryptographically secured by algorithms. It uses some type of blockchain technology or other distributed ledger technology (DLT) and can be transferred, stored or traded electronically[2].

A cryptoasset inherits all of a blockchain's good features, such as being programmable, open, immutable, borderless, decentralized, permissionless and available around the clock. It can be used by humans as well as software agents and machines such as internet of things (IoT) devices, making it possible to turn any traditional, physical asset into a digital one.

Tokens using blockchain can represent new, native assets such as bitcoin, or non-native assets that are backed by traditional assets such as the following (see **Figure 1**):

- Stablecoins representing fiat currencies, like Tether tokens, which are backed one to one by the U.S. dollar, and Libra, the prospective Facebook coin backed by a basket of currencies
- Metals, like Digix's DGX, which represents one gram of gold secured in a custodial vault
- Real estate, where property owners issue tokens on blockchain-powered platforms representing a number of shares of real estate assets such as those issued via startups Harbor, Galaxy Digital Holdings, Propellr, Fluidity and Blockchain App Factory

[1] https://coinmarketcap.com/

[2] Taskforce, C. (2018). Cryptoassets Taskforce: final report. HM Treasury, Financial Conduct Authority and Bank of England.

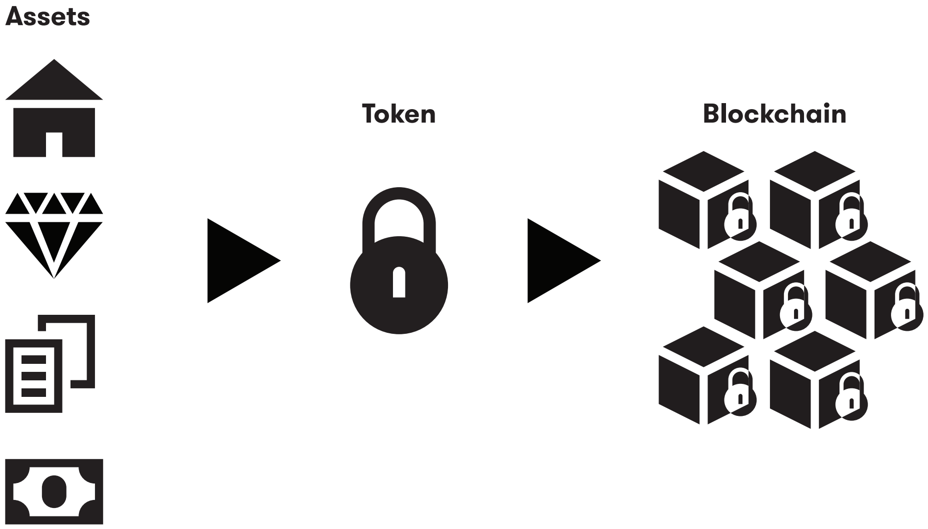
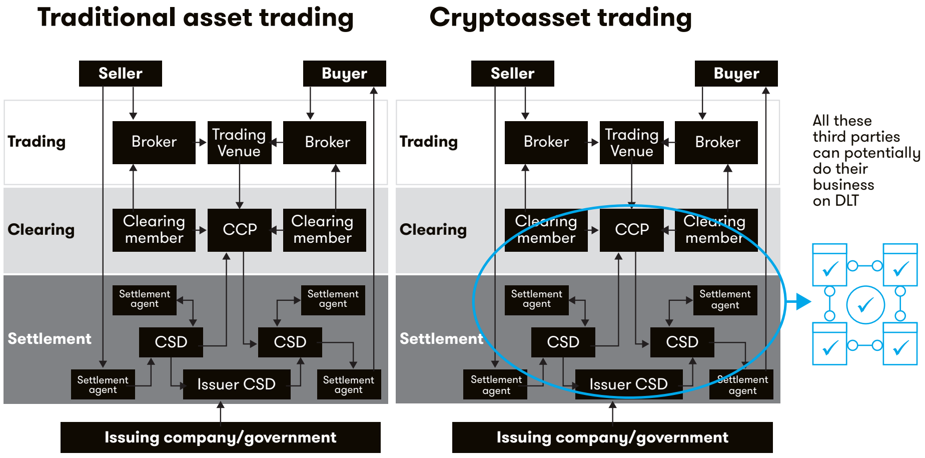


Figure 1. Asset tokenization

Disrupt trading with tokens

Capital markets transactions involve trading, clearing and settlement processes and many third parties — brokers, trading venues, clearinghouses, settlement agents, custodians and issuers, as illustrated in **Figure 2**. Establishing and running these third-party organizations is costly, complex and requires executing complex and long business processes to ensure integrity and the protection of the stakeholders. The one-time cost of the issuance of an initial public offering (IPO), for example, can reach more than $1 million[3], with a recurring annual cost of up to $1.9 million.



All these third parties can potentially do their business on DLT

Figure 2. Trading traditional assets vs. cryptoassets[4]

[3] PWC. (2017, Aug 06). Considering an IPO to fuel your company's future? Retrieved from https://www.pwc.com/us/en/services/deals/library/cost-of-an-ipo.html

[4] Pinna, A., & Ruttenberg, W. (2016, April). Distributed ledger technologies in securities post-trading. Revolution or evolution? European Central Bank. Occasional Paper Series. No 172.

Blockchain technology has the potential to cut costs and streamline the clearing and settlement processes by replacing third parties and eliminating the need for their existence or reducing their roles — all while maintaining integrity and protections. It also opens the door to decentralized trading, either peer-to-peer or through decentralized exchanges.

Using this technology, asset ownership can be easily issued, verified and transferred on the blockchain. The actual settlement can be either done immediately or almost in real time if the assets are native. For non-native assets, it may require a custodian or settlement organization to reflect/apply the final settlement.

The following table compares trading traditional assets versus cryptoassets and the main players in the trading value chain:

Activity	Traditional asset trading (example: stocks)	Non-native cryptoasset trading (off-the-blockchain assets, such as STO tokens)	Native cryptoasset trading (on-the-blockchain such as bitcoin[5])
Trading	Centralized exchanges	• Peer-to-peer trading • Centralized STO exchanges • Decentralized STO exchanges	• Peer-to-peer trading • Centralized exchanges • Decentralized exchanges
Clearing	Clearing organizations	Clearing organizations and protocol	Software protocol
Settlement	Custodian/ settlement organizations	Custodian off-blockchain and protocol	Software protocol

How cryptoassets enhance financial services

Asset tokenization in financial services using blockchain technologies can revolutionize and solve problems around payment, investment, trading and raising capital. It helps financial services companies:

- **Reduce friction and overhead costs** associated with issuing, transferring and managing traditional assets such as securities, commodities and real estate assets. Tokenization eliminates many third-party processes, reduces costs and facilitates trading and settling assets in real time.
- **Increase liquidity** by designing divisible cryptoassets for real estate or any traditional asset and making them widely accessible on trading venues. Divisible cryptoassets mean a large number of people can each own a fraction of a piece of property or another asset. Furthermore, tokenized assets available on one exchange are easily available for trading on other exchanges. In fact, exchanges commonly share their order books with liquidity providers, which in turn open the door to making the assets available on global markets. Asset price information spreads across exchanges more quickly and efficiently, resulting in better pricing by narrowing bid/offer spreads and improving price discovery.

[5] Pinna, A., and Ruttenberg, W. (2016, April). Distributed ledger technologies in securities post-trading. Revolution or evolution? European Central Bank. Occasional Paper Series. No 172.

- **Simplify regulatory compliance** by automating rules and enforcing them through code in smart contracts on the blockchain. Compliance that is complex and costly in the physical world — for example, limiting the number of owners and their shares and enforcing their rights accordingly — is easy to implement and enforce in the blockchain smart contract.
- **Increase transparency** throughout the asset life cycle by leveraging blockchain's inherent transparency and trust. Blockchain transactions are available, verifiable and auditable. In public, permissionless blockchains, the transaction ledger is accessible to any user. In private, permissioned blockchains, it is available only to the participants in the network.
- **Create new business models and new incentives** by virtualizing any value or valuable activity and facilitating easy transfer among participants, thereby encouraging them to create more value. In addition, building tokens on top of a decentralized network can eliminate traditional third parties and disrupt their models. Basic attention token (BAT), for example, aims to disrupt traditional digital advertising[6] by allowing the value — in this case, user attention — to be exchanged peer-to-peer among publishers, advertisers and users.

Start with design challenges

Designing a new cryptoasset or tokenizing traditional assets is complex and requires addressing business, legal and technology challenges.

Business challenges

Understanding the problems being solved by tokenization is key to designing the role of the new cryptoasset and its use cases. Key players in financial services classify cryptoassets into three categories[7] based on the role they play (see **Figure 3**):

- **Exchange cryptoassets** such as bitcoin and litecoin, also called cryptocurrencies, are used mainly as payment to buy and sell goods and services, to facilitate decentralized, peer-to-peer settlement or as an investment.
- **Security cryptoassets** are used mainly as investments held and traded for capital gains. They represent ownership, shares or other investment-related rights. People use them as tools to raise capital in equity and public share offerings.
- **Utility cryptoassets** are used mainly to access specific services provided or hosted on a blockchain platform. Think of them as a paid API key (but not an API). You can buy an API key from Amazon Web Services and then redeem this API key for time on Amazon's cloud. Similarly, on a blockchain such as Ethereum, you can use a utility cryptoasset to access a decentralized computing platform.

[6] Brave Software. (2018, MAr 13). Basic Attention Token (BAT) Blockchain Based Digital Advertising. Retrieved from Basic Attention Token: https://basicattentiontoken.org/

[7] Taskforce, C. (2018). Cryptoassets Taskforce: final report. HM Treasury, Financial Conduct Authority and Bank of England.

Some cryptoassets can be classified under more than one category based on their use cases. For instance, some cryptoassets commonly used for payment are also used for investment. Ethereum's open public blockchain network, which provides access to decentralized computing to run smart contracts as a utility to issue offerings, is also used for payments and, in a few cases, investments.

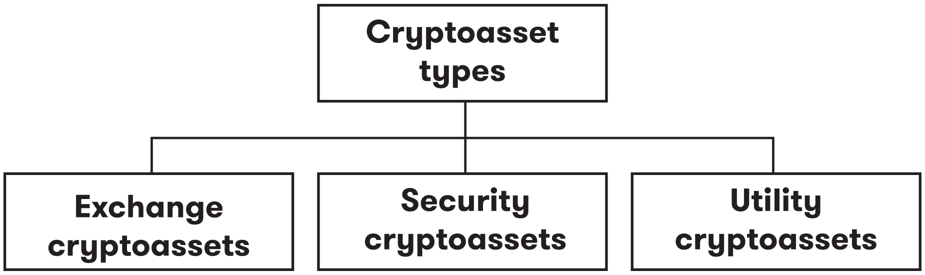


Figure 3. Cryptoasset classifications

Legal challenges

Cryptoasset design requires asking questions about the regulatory frameworks involved, asset ownership and the location where assets will be issued and traded. Certain regulations are global — such as the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act — and affect all types of financial services. Other regulations vary with the token type, its use case and the location of the owner or the entity managing the asset.

Technology challenges

Addressing the technology challenges is crucial to the success of the new cryptoasset. It requires dealing with important technical decisions such as technology/vendor evaluation and selection, and solution design and implementation. Designing cryptoassets requires trade-offs among three dimensions: performance, resiliency and privacy. These decisions may force trade-offs[8] that focus on one dimension at the expense of the other two:

- **Resiliency vs. performance.** A blockchain network increases its resiliency against faults and attacks by adding more nodes to its network. This provides redundancy by having the data available on multiple nodes, but at the expense of performance.
- **Privacy vs. performance.** Privacy in blockchains is implemented by limiting the data distribution in the network: (1) creating different subledgers available to a limited number of participants or (2) implementing encryption algorithms that are computing intensive. Both options negatively affect the network's performance.
- **Privacy vs. resiliency.** Resiliency in blockchains is best achieved by having all data available in one common ledger that is available to all participants via a large number of nodes. Limiting access to implement privacy requirements necessitates different subledgers and/or complex encryption algorithms that negatively affect the resiliency of the network against faults and attacks.

[8] Taskforce, C. (2018). Cryptoassets Taskforce: Final Report. HM Treasury, Financial Conduct Authority and Bank of England.

Achieve goals with a phased approach

A phased approach methodically and thoroughly addresses specific business and technical goals and requirements for the cryptoasset journey. There are five key phases (see **Figure 4**).

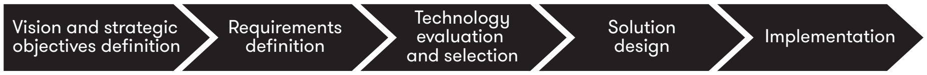

Vision and strategic objectives definition
Requirements definition
Technology evaluation and selection
Solution design
Implementation

Figure 4. Five phases for delivering a cryptoasset solution

Phase 1: Define the vision and strategic objectives

Building a vision and understanding strategic objectives involve identifying the cryptoasset's goals and the features needed to implement them.

1. Determine the cryptoasset's type and objectives. If it is an **exchange** cryptoasset to facilitate a payment, ask:

   – Is it for wholesale or retail payment?

   – Will it work with traditional payment systems, such as real-time gross settlement (RTGS), Enhanced Bidding Power Scheme (EBPS) and automated clearinghouse (ACH) systems, or with public crypto-networks and systems, such as Bitcoin and Ethereum?

Most central banks are exploring blockchain technologies to design and implement digital currencies for payments. And many large financial services firms have built stablecoins (a digital version of fiat currencies).

If it is a **security** cryptoasset for an investment, ask:

- What asset does it represent?
- Is it native or non-native?
- What kind of rights to ownership or shares does it represent?

Many financial service firms are building security tokens for various purposes.

If it is a **utility** cryptoasset, ask:

- Is it for accessing specific simple products or services, such as basic computing resources — CPU, memory or bandwidth?
- Or is it for accessing a complex product or service such as artificial intelligence (AI), advertising, messaging or market prediction?

2. Identify the main use cases — the set of possible interaction sequences between the cryptoasset and its users to achieve a particular goal: payment, investment, access or raising funds. These cases are the foundation for identifying all actions or events that define the interactions.

3. Explore the key features:

   – **Privacy.** What are the privacy requirements of the new cryptoasset? Are the transactions public or private? If private, are they private to all stakeholders, or are there specific privacy requirements for each stakeholder group? In some digital assets, for example, such as central bank digital currencies, regulators require access to all information, while other stakeholders have limited access related only to their transactions.

- **Asset issuance process.** Will this new asset be issued publicly or privately? Cryptoassets are issued publicly in two ways:

  » Via an *offering* process called either an initial coin offering (ICO), initial exchange offering (IEO) or security token offering (STO), depending on the cryptoasset's type and use cases. There are many differences between these offering processes, but the main difference is who is managing the process: Is it the entity creating the asset (for an ICO), an exchange where the assets will be listed and traded (for an IEO) or the authority regulating the capital market (for an STO)?

  » Via *mining*, a process that rewards participants who solve a computational problem that secures the network with newly issued cryptoassets. All proof of work (PoW) public blockchains, including bitcoin, use mining.

  Private or nonpublic offerings are possible and usually done with stablecoins and central banks' digital currencies. Some cryptoassets, such as Zcash, are issued as partially open and partially private.

- **Decentralization level.** Cryptoassets vary in the level of their decentralization — how much the asset's key functions and features are distributed or delegated away from a central, authoritative participant in the blockchain network. Some cryptoassets, such as bitcoin, are highly decentralized; some, such as stablecoins, have a low degree of decentralization and others, such as Ethereum, EOS and Ripple, are in between.

- **Asset supply.** Gold and other traditional assets used to back cryptoassets must be fixed and match the amount of the reserves backing them. In addition, issuers can apply issuance rates or specific rules.

  Some public cryptoassets fund their development or community by taking a portion of the issuance rate. Zcash, for example, has a Founders' Reward[9] where, over the first 4 years of its issuance, 10 percent of its total 21 million token supply of Zcash goes to the founders and the remainder to the miners on the network.

- **Other features.** Decisions in cryptoasset design also include:

  » Fungible or nonfungible: Fungibility means that the individual units of the cryptoasset are essentially interchangeable and its parts are indistinguishable.

  » Divisible or nondivisible: Divisible assets can be divided into smaller units. Some assets are nondivisible, such as those used in games (CryptoKitties, for example).

- **Asset trading.** If the asset is tradable, where is it going to be traded? How will it execute the clearing and settlement processes? Is there a role for a custodian third party?

[9] Hopwood, D., Bowe, S., Hornby, T., & Wilcox, N. (2018, March 19). Hyperledger Fabric CA (Certificate Authority). (2017). Retrieved from Hyperledger fabric documentation: https://hyperledger-fabric-ca.readthedocs.io/en/release-1.4/

Phase 2: Define the requirements

After defining the cryptoasset's vision and objectives, clarify the requirements. Functional requirements spell out exactly how to execute each process in the cryptoasset's life cycle:

- **Issuance:** How will the asset be issued — publicly (ICO, IEO or STO) or privately? If it is backed by other assets, how will the pledging process ensure that the issued amount matches the pledged or reserved amount?
- **Transfer:** What is the transfer process among participants? Can it be initiated from any participating node or only from specific ones? Are there any rules governing the transfer? Do transfers need approval?
- **Trading:** If assets are tradable, how will the trading cycle (trading, clearing and netting) be executed?
- **Destruction:** What happens to the asset when it needs to be destroyed? Will any backed assets need to be redeemed?

Nonfunctional considerations include security, availability, scalability and performance.

Securing cryptoasset systems and the blockchain network is particularly crucial and involves node access control, smart contract security, performance and scalability.

Phase 3: Evaluate and select the technology

After clarifying the cryptoasset's objectives and requirements, it's time to determine which blockchain technologies best fit the functional and nonfunctional requirements. Building a new blockchain from scratch is an option, but it requires substantial effort and time.

Cryptoassets that need a high level of decentralization can be built using one of the many public blockchains. These blockchains serve a wide range of purposes and specifications.

Public blockchain systems are either permissionless, where anyone can join (such as Bitcoin and Ethereum), or permissioned (such as Ripple and EOS), which require permission from one or more of the entities governing the network.

Private and permissioned blockchains work well for cryptoassets needing privacy among a closed number of network participants (central bank digital currencies, for example). Quorum, Hyperledger Fabric, and Corda dominate the private and permissioned blockchains on the market today.

Phase 4: Design the solution

Developing an architecture for cryptoassets solutions calls for solution design decisions on components in several areas, including:

- **Privacy and confidentiality.** Many technologies can support privacy in blockchain such as Channels and Private Data Collections in Hyperledger Fabric (HLF), Zero Knowledge Proof protocols (ZKP) in Quorum or Flows and Settler in Corda.

- **Role of consensus protocols and nodes.** There are many consensus protocols used widely, such as Proof-of-Work (PoW), Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT). Each one of these protocols is suitable for a specific set of scenarios and functions.
- **Asset transfer protocols.** Asset ownership transfer can be done either natively on-chain or cross-chain. Cross-chain transfers (called atomic swaps) can be designed and implemented using Hash Time Locked Contracts (HTLC) protocols.
- **Asset custody and storage.** It is all about how to store and secure the cryptoassets. Cryptoassets backed by traditional assets may require third parties' custody service providers.
- **Token-based vs. account-based.** Blockchain uses both models to keep track of cryptoasset balances and prove their ownership. The token-based model is more scalable and offers a higher level of privacy, whereas the account-based model is more suitable for scenarios that require less privacy and more efficiency.
- **Smart contracts.** Smart contract programs contain the code that carries out the functions and enforces the rules governing the cryptoasset. Therefore, they are the most important design element.
- **User interface and wallet user experience (UX).** The user interface for the application interacts with the blockchain where users execute functionalities on the cryptoassets.
- **Security.** Key security design issues related to cryptoassets include how new nodes in the network are permissioned. They can be either PKI-based, where a certificate authority issues digital certificates for permissioned nodes, or based on a smart contract's whitelist of node addresses. The other design issue is how to secure private keys in the nodes participating in the network. A common industry practice is to require hardware security modules (HSM).
- **Integration and APIs.** Cryptoasset data may need to be exposed through APIs. Designing a cryptoasset as an ecosystem requires opening the specifications of the system to other users, such as developers, service providers, exchanges and payment providers, to allow them to build other products and services on top of the new cryptoassets.

Phase 5: Implement the solution

The implementation phase involves developing and deploying the designed components, making sure they are tested and that they fulfill the business, functional and nonfunctional requirements.

Cryptoassets have the potential to deliver significant benefits for financial services organizations, including opening up new business models, streamlining processes, simplifying compliance, reducing the number of third parties, lowering costs and increasing transparency.

Designing these new assets is complex, however, and requires tackling many business, technical and legal challenges. It also involves grappling with difficult decisions, including possible trade-offs in performance, resiliency and privacy.

A phased approach to designing and implementing cryptoassets provides clarity for the journey and makes sure organizations address all of the many aspects involved.

A world of possibilities

The possibilities from tokenizing traditional assets, or even developing new cryptoassets, are vast. If the benefits and potential use cases align with business goals, financial services organizations would be wise to consider entering the exciting new world of blockchain and cryptoassets.

About the author

Alsaiyed Haiyan, a FinTech and blockchain advisor at DXC Technology, provides consulting services around designing and implementing cryptocurrencies and cryptoassets, central bank digital currencies, crowdfunding, crypto market trading, investment, FinTech regulations and payments.

About DXC Technology
DXC Technology, the world's leading independent, end-to-end IT services company, manages and modernizes mission-critical systems, integrating them with new digital solutions to produce better business outcomes. The company's global reach and talent, innovation platforms, technology independence and extensive partner network enable more than 6,000 private- and public-sector clients in 70 countries to thrive on change. For more information, visit **www.dxc.technology**.