



Tokenization

Establishing Digital
Representations of
Value as the Medium
of Exchange

Contents

Introduction

1

Token Basics

3

Authenticity

4

Token Properties & Behaviors

6

Token Taxonomy Terms & Concepts

7

Important Token Concepts

11

Real-World: Use Cases

13

Summary

15

© 2019 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

Introduction

Digital tokens are not entirely “new”. Use of a token as authorization to perform a task, access some resource or as a license to listen to or watch digital media are some examples you may be aware of. Some industries like the financial services have been creating digital securities for decades. However, hidden in plain sight, at the core of one of the most hyped and misunderstood technologies, blockchain, ***lies an immensely powerful concept that will forever change the way transactions between parties execute.***

Tokenization, the process of tokenizing all sorts of items or assets used every day or in the future, is still in its infancy and can be confusing at first. However, stepping back from the hype and technobabble, it is possible to achieve a clear understanding of how to harness it and participate or even lead in this revolution without having to know the ins and outs of blockchain technology. A good business sense will do.

There are currently two token “universes” at the moment in the form of public and private or consortium blockchain networks.

1. A public universe heavily tilted towards crypto currency use cases that features a diverse and wide selection of blockchain choices, each of them differentiating themselves on their technical underpinnings and evolving new economic models.
2. An enterprise or corporate universe that provides a narrower choice of blockchain technologies focusing on evolving existing economic models with a more diverse and wide view of tokens.

At some point the boundary between these two universes, public and private, will blur as the technology and social, economic, legal, regulatory and practical aspects involved with this disruptive technology matures. But for now, it’s safe to think that the use of tokens in the public universe is narrowly focused on different versions of money or crypto currency and the private universe is widely focused on tokens that are not.

Blockchains or Distributed Ledgers have three basic building blocks: Tokens, Contracts, and Identity or identifiers, that are used to build multi-party applications. The blockchain represents a shared “truth” by establishing authenticity using agreed upon cryptographic techniques to create digital representations of Tokens, Contracts and Identity.

A shared ledger uses cryptography that is trusted by multiple parties to authentically represent tokens or assets of value that can be owned by accounts belonging to the parties that trust it.

The concept of Tokenization should be more of a business construct than a technical implementation. You certainly need to have an implementation to make tokens real, but you do NOT need the technology to conceptualize what tokenization means and how you can use it to transform your business.

In this paper, we will focus only on Tokens, what they are and how they can be used. A solid understanding of the concepts as it applies to everyday business problems is vital to achieving a successful technical implementation of your tokenization strategy.

Token Basics

Bitcoin, a token that is also a cryptocurrency, was the first blockchain application and is an indication of just how foundational tokens are to blockchains. A token is a digital representation of value, where the representation is agreed to and trusted by all participants in the blockchain network.

What value is the token representing? Well, that varies based on the business requirements for the representation. Generally, tokens can represent a wide variety of things.

For example, think about the board game Monopoly - the game is full of tokens. A game piece that each player chooses to represent themselves in the game is a token representing the player. Then there are the property cards that are tokens of the physical property. And the money the players earn and use to purchase those properties and the "Get out of Jail" card a player can draw when they get into trouble...all tokens.



Each of those things represents a token, but these tokens are not of the same type, nor do they all have the same behaviors or properties. A game piece represents a player, like their identity or account. Monopoly money represents physical money and the property cards represent a land deed or title.

Authenticity

The single most important thing about any token, regardless of its type, is its authenticity. Fewer aspects of value are as emotionally charged as believing in the authenticity of value by its owner. Fakes, forgeries, counterfeits and knockoffs are example terms used when evaluating the origins of value.

For example, if you have a \$100 bill with a serial number of **H4829310239** and come across another \$100 bill with a serial number **H4829310239**, one of them is a counterfeit. But which one?

How much is your \$100 worth now? \$50? No, it is now effectively worth \$0 – since you can't trust the dollar bill you are holding.

A token's value is a zero-sum game of confidence.

Absolute authenticity or the extreme unlikelihood of being able to produce a convincing counterfeit, is vital for achieving and maintaining value over time.

How do we achieve and sustain authenticity in the era of “fakes”? Let's look at some historical examples.

The Dawn of Currency

A simple way of establishing and determining authenticity is to have the token represent the value intrinsically, meaning the token is the value itself, like a gold coin.

The authenticity of gold coins was initially determined dentally, i.e. physically biting the coin, which at the time was risky for your gleaming smile if a counterfeit broke a tooth as the dentist was also likely the town blacksmith. The practicality of intrinsic value tokens when the token is a physical coin was short lived. Gold coins were of great value in of themselves but came with a lot possession risk that often led to problems dwarfing the state of your dental health.

An interim step of plating low value materials with precious metals such that their relative value was greater than their melted form was dependent on non-inflationary conditions. Ultimately full on material substitution to make the coin completely out of low-valued metals and even paper notes, that represented a stored value of gold became acceptable.



These tokens, coins or notes, represented a certain quantity of gold held in the issuer's coffers, safe or vault, the bearer of the coin or bill could request from the issuing institution the amount of gold it represented in exchange. This complete substitution of value changes what is needed to determine authenticity of the token when exchanging it with another party.

This is often called the Gold Standard, which technically it's not, regardless this token scheme was the trust anchor underlying fiat currencies around the world until the early 1970s. The bearer of these instruments trusted that the institution that issued it had the gold to back it up, so all they had to worry about was that the instrument itself was authentic.

So how did the issuers of these tokens establish trust and allow for their users to determine authenticity?

Minters of coins and issuers of paper currency employed difficult to duplicate properties, that could almost instantly calm any concern by its holder as to its authenticity. The molds or plates used to generate these instruments had fine detail that at the time of their issuance was difficult to duplicate in order to create an effective counterfeit at scale.

Counterfeiters would experiment and eventually be able to create good enough instruments, or just steal the molds or plates. This would then cause a new series of instruments to be created, moving the difficulty bar further out. This continues to this day, all around the world.

Determining authenticity wasn't just an issue to the general public, but to governments and the minters they employed. The United Kingdom, in the twelfth century, began regular inquisitions called the [Trial of the Pyx](#) for the minter to prove conformity to a jury of metallurgical assayers, a.k.a. inspectors, just in case they were skimming or creating extras. This too continues to this day.

Perhaps the most interesting aspect of today's currencies is that they are not backed by gold, but trust in the backing government and authenticity. This, to most, is magic, but the authenticity challenge persists.

Token Properties & Behaviors

With coins and paper notes their physical properties are used to establish authenticity. It usually can be determined immediately and can be verified with further scrutiny by its properties like paper quality, holographs, serial number, etc.



Interestingly, the amount of intricate detail implemented can make it easier to fool people into accepting counterfeits that are deemed to have the same level of intricacy at first glance.

Blockchain tokens achieve their authenticity using a combination of cryptography and an immutable distributed ledger (blockchain network). Understanding how this combination works is not important regarding the design and use of tokens. The cryptography is mathematics which your computer can perform with a much greater degree of accuracy than you can calculate the paper weight of a stack of paper bills.

The computer program, and potentially a device, you will use to hold and use your tokens is called a **wallet**. One of its primary jobs is to validate both the network and cryptography of the token so you will not be using counterfeits.

Behaviors

Tokens behave in certain ways like:

- Subdivide into smaller denominations, or making change
- Coalesce into larger denominations, for example, converting a bucket of coins into a much lighter bill
- Interchangeable value with any other money of the same denomination
- Support supply control, central banks can “print” more money and remove older series that are susceptible to counterfeiting or to implement [monetary policy](#)

These concepts should be familiar to most readers, however, the words and terms used to describe them can often seem like “token jargon”. So, to explain these concepts more, we will use the terminology and definitions defined in the open standard maintained by the [Token Taxonomy Initiative](#) (TTI) called the Token Taxonomy Framework (TTF).

Token Taxonomy Terms & Concepts

Fungible

Understanding physical money provides a good baseline for fungible tokens. These tokens have interchangeable value with each other, meaning that any quantity of them and their sum will have the same value as another quantity with the same sum. This can be nuanced in some scenarios which require quantities be in the same class or series.

Put very simply, a pile of cash equal to \$1,000 made up of ten \$100 bills has the same value as \$1,000 comprised of all pennies (\$.01). In this case, the burden of carrying ten pieces of paper vs. 1,000,000 coins could make a difference in relative value if you must carry it around.

Physical cash consolidation by money changers (central banks and their commercial arms) provide services to convert your subdivided bits into whole larger bits equal in value, for a fee. Today this conversion is usually physical to digital in the form of a deposit or vice versa.

Non-fungible

A non-fungible token is not interchangeable with other tokens of the same type, because they typically have different values. A car title is a good example of a non-fungible token. For example, a title to a 1971 Ford Pinto does not have the same value as one for a 2019 Porsche 911.

Baseball cards, Comic Books, Art, and [CryptoKitties](#) are other examples.

Hybrids

With digital tokens you can create parent, child relationships to model out different business scenarios. For example, you can have a non-fungible parent with a child token that can be fungible, representing a general admission concert ticket, where the parent token represents the specific date of the concert and the child being one of a fixed number of general admission tickets. This concert could also have reserved seating represented by a second child token(s), one per seat as each reserved seat can have a different value. Better seats have higher value. All the child tokens are only good for the date of the concert and cannot be used for the next day.

You could also have a fungible parent with a pool of non-fungible tokens where each fungible parent token owns a fraction of the non-fungible tokens.

Mutual Funds and mortgage backed securities are other good examples of hybrid tokens, where the fungible security (token) can be the owner of a bunch of other securities or non-fungible mortgage tokens. The parent can have a fixed number of instances and be owned or sold to a bunch of investors where each token owns a fraction of the securities or mortgages owned by the class.

Token Template

Templates are like a recipe for creating a token. It describes the token based on its type and what capabilities or restrictions a token created from the template would have.

Token Class

This is a deployed token from a template, i.e. Bitcoin is a token class that collectively represents all Bitcoins. The definition, capabilities and restrictions of the class can be understood from the template it was created from. This is not a concrete example, since Bitcoin was the 1st blockchain token, there were no standards like the TTF to define what a cryptocurrency was at the time.

Token Instance

A single token in a token class, i.e. a single Bitcoin, or any fraction of one, you could have in your wallet that belongs to the Bitcoin class.

Token Properties

Tokens usually have a common name, a symbol or unique identifier, a quantity and an owner. These values belong to the token class where instances of this token will have these same values.

There can be other values like a serial number or a SKU that are nuanced so we will revisit them later in a context where it's easier to understand.

Token Behaviors

Behaviors are capabilities or restrictions and can be common across fungible and non-fungible types or only apply to one of them. Behaviors can have supporting properties which they incorporate within themselves.

Behaviors and the combinations of them provide the flexibility to create a token that models a business need. Behaviors are very business specific and usually have existing "non-blockchain" implementations which are well understood.

Here are some common behaviors.

- Transferable – the ability to transfer ownership of the token. Basic fungible behavior when using cash money, but also applies to non-fungible tokens.
- Non-transferable – the restriction of preventing a change of ownership from the initial issued owner. A vote token for an election or an airline ticket are examples.
- Sub-dividable – these are essentially the decimal places a token can be subdivided into. For example, a dollar supports 2 decimal

places. A zero decimal would prevent subdivision or the ability to own a fraction of a token, these are referred to as whole tokens.

- Mintable – the ability to issue new tokens of the class. Creating money or barrel of oil to add to the overall supply of the class.
- Burnable – the ability to remove tokens from the supply. A token representing a barrel of oil that gets burned when it is refined is a good example.
- Role Support – the ability to have roles defined within the class can allow or prevent certain actions.
- Financable or encumberable – the ability to have another token or contract prevent the transfer of ownership or burning until the encumbrance is removed. For example, an outstanding loan on a property that is encumbered will require that the loan be paid off before the ownership of the property can be transferred.
- Expirational – the token loses its value based on an event or date. A ticket to the theater is only good for the date of the play and is not valid for the next day's show.
- Suspendable – a token can be restricted for redemption, transfer or use based on some event. A token that represents a credit may be suspended until some issue with the credit is resolved.

There are many more behaviors and properties that are defined by vertical industry specialists and are integrated into the open standard maintained by the TTI.

For example, industry specific token properties like a SKU, Serial Number or industry identifiers (CUSIP, Ticker, codes) that you might want to ensure your token exposed and could be queried for.

The same goes for industry specific behaviors like financeable, insurable, perusable, renewable, etc. where the industry experts in finance, retail or energy define what it means when a token has one or more of these behaviors.

These properties and behaviors become the building blocks for creating industry integrated, interoperable and all sorts of cross vertical industry possibilities.

For example, suppose you were creating a token that represented a proof of purchase/ownership for an item you manufactured. Your customers want to be able to insure this item with their insurance provider. Without the TTF, it would be your responsibility to contact their provider to find out what data elements they can provide to link

your token to their insurance policy. But you would have to do this for ALL the possible insurance providers. With the TTF, the insurance industry defines the insurable behavior and you can simply reuse it in your TTF definition and snap to the insurance standard effortlessly.

The [Token Taxonomy Framework](#) goes into much more detail about the different token behaviors and properties and provides tools for you to quickly model a token for your business needs as you prepare for implementation.

Important Token Concepts

Tokens are rapidly becoming the representations of value exchanged by parties on business networks. Representing everything from bank balances or fiat currency, product inventory, supply chain documents, receipts, tickets, authorizations, gaming assets, loyalty points, subscriptions, etc. Some concepts should be broadly applied when thinking about how tokens could be used in your business.

- The owner has complete control of it, unless you have defined specific restrictions such as recallable or pause-able where the token issuer can override the owner of the token to suspend use of the token.
- A token instance, whole or fraction, is a single party unit. Meaning, it usually has a single owner and is transacted against in a single transaction. There are scenarios where you may want multiple owners, sometimes called multi-signature tokens.
- Tokens are meant to be contracted. A transfer on a token will not be aware of any conditions that need to be met before completing. A token receiving a transfer request is not concerned about the external conditions in which the transfer was generated. But the token can have a behavior like *financeable* which allows a contract to encumber the token to prevent the transfer to another party until the loan or lean is removed. The token doesn't need to be aware or concerned about how it was encumbered or how it is freed, that is the loan, or contract's job. This allows tokens and contracts to interact with each other seamlessly.

A token's behaviors provide an interface or extension for how the token can be used. For example, if a token is financeable, it has the ability for the owner to accept a lien, representing the loan, which encumbers the token. In this case, the loan represents a contract that is bound to the financeable behavior of the token. The loan itself is a multi-party contract with the token owner being the borrower and the financier the lender. The token and the loan operate independently, however only the loan can remove the lean once it is paid in full.

This brings us back to the important point that tokens are not multi-party contracts, or at least they shouldn't be. ***Defining and implementing contract logic along with the token decreases the token's re-use and interoperability.*** Tokens are meant to represent value which are referenced in multi-party agreements or contracts.

For example, a property title token should be encumbered by a loan contract which defines the lender and conditions needed to be met to remove the lien from the property. The token and the contract are separate but can integrate with each other. If the property is sold by the

owner and the buyer wishes to finance the purchase, a new loan contract can encumber the property title token as the older encumbrance is removed.

A Token behavior can act and react to itself or require an external actor like a contract to invoke it, or its internal and external behaviors. Technical people usually call this an interface, but you can think of an external behavior like an electrical outlet and the thing you are plugging into it is the contract or even another token.

Real-World: Use Cases

Let's look at some real-world use cases for tokenization. Most people are familiar with cryptocurrencies, but they might not understand how they work and using them seems complicated, so we will not spend time explaining that. Rather let's look at some existing business models where tokens are in use today.

Loyalty

Loyalty points are everywhere, from your local grocery store, a hotel chain, airlines, to your favorite barista. This model allows for the issuer of a "point", which we will now call a token, to establish the value behind token. A hotelier can price room upgrades in tokens, airlines will price flights, etc.

For the most part, these points exist in walled gardens, you're not likely to be able to exchange points from one garden to the next without some significant effort between the gardens to figure out how to do the exchange. Much of the effort can be attributed to technical infrastructure with the rest being legal and figuring out exchange rates and settlement.

Blockchain networks can establish environments where the walls between gardens can be removed and the TTF would allow for valuation, exchanges and settlement to be defined enabling a common implementation.

Supply Chain

Supply chains represent a fertile ground for innovation using tokens and contracts. Tokenizing inventory and packaging of physical goods allows for tracking and tracing goods as they pass through the supply chain.

There is a lot of paper documentation that is generated when ordering, fulfilling, shipping, receiving and invoicing between parties. Each of these steps could tokenize key documents like an Order, Bill of Lading, and Invoice, storing digital copies of the printed paper for archive and recall and linking it to a token that represents that actual document.

However, there is much more that could be done. A buyer may need to acquire financing to place an order and the seller may also need financing to fulfill the order. And when the order is fulfilled, the seller will want to invoice the buyer to complete the transaction and cascade it to the finance components.

By tokenizing the documents, the financiers can define a behavior called financeable that the buyer and seller can include in their token definitions so when financing is provided to the buyer or seller, the documents will be directly linked to the finance contracts removing the need for manual correlation at settlement time.

The same thing goes with insuring goods as they move between the seller and buyer. Tokenization of a bill of lading could implement the insurable behavior to make this seamless and drive further automation.

Summary

Applying standard ways of defining tokens in a modular way, using well understood business models across industries can lead to a vastly improved business ecosystem. Sharing of token definitions across industries can drive integration and automation improvement in what are highly manual processes today.

Tokenization is a pillar of the coming revolution in multi-party applications that blockchain technology ushered in. There are enormous possibilities for peer to peer value transfers that are much more efficient, easier to regulate and trust, but in order to get there you must be more deliberate in designing how value is represented.

At Microsoft we believe that supporting and following open standards for creating Token definitions and specifications with organizations like the Token Taxonomy Initiative and encouraging verticals to share and reuse across the board is a huge step in the right direction.

Having a clear definition and agreement for how value is represented on these blockchain networks that can be understood by everyone, not just blockchain developers, can allow for existing business processes to be streamlined and new ones to emerge. New business models defined in this way will have integration and reuse baked in from day one.

However, there is more that needs to be done here. Implementation of standard token specifications and the ease in which they can be used has a long way to go. Tokens need to be as easy to use as the everyday, “real world” ones are today. Using a crypto currency should be as easy as using cash or a credit card. Building an application that allows for customers to shop and acquire insurance across many providers for shipping high value goods across an ocean should be simple.

Using a token should be like driving a car. If you know how to drive one, switching to a different make, model, engine or fuel doesn't require the driver to learn a new gas and brake pedal or how to use a steering wheel.

At Microsoft, we are busy closing the gap from the common cross vertical token standard to an easy to use, extensible and cross blockchain network world, bringing tokenization to the masses.