UNIVERSITY *of* NICOSIA

Week 1, Session 2

Blockchains and Examples

BLOC 528: Token Economics

Key Terms

Authentication is the process by which a person, institution, or object is proven that it/they is consistent with the claim. Digital identities with claims and credentials are used.

A decentralized identifier is a public and pseudo-anonymous unique digital identifier for a person, company, or object that grants personal control to one's digital identity without the need for centralized institutions managing the identifiers. They need to be permanent so they cannot be reassigned to other identities.

A Public Key Infrastructure is a cryptographic system relying on Private Keys (typically only known to a single key holder, and the associated Public Keys that are well known and that can typically be associated with a key holder. A PKI allows both for Encryption and Digital Signature of communication. Similar in application is a Symmetric Key Infrastructure that relies on a shared secret for the same purposes.

A distributed consensus refers to a consensus about the current state of the world (as defined by the contents of a database, or a subset thereof) amongst different actors that are usually spatially separated (and therefore take a measurable time to communicate) and might are might not be willing to honestly cooperate.

Byzantine Fault Tolerance refers to the ability of a system to continue to function even if a certain number of participants acts dishonestly, with an intent to manipulate or disrupt the state of the system.

Key Terms

A Sybil Attack is an attack on a system where one node impersonates multiple nodes (for example by voting multiple times). Proof-of-Work refers to a system that protects itself against those attacks by making voting costly, proof-of-stake to one where the protection comes from participants staking scarce resources that can be seized in case of dishonest behavior, and proof-of-authority refers to a system where the participants identify themselves using credential from the 3rd party authority (e.g., they show their passport).

Proof of work is a consensus mechanism where we approximate the selection of a random node by selecting nodes in proportion to a resource that is hoped that nobody can monopolize upon. Nodes can “compete” with one another by using their computing power to solve mathematical problems. To create a block, the node that proposes the block is required to find a number (nonce) such that when you concatenate on that nonce, the previous hash and the list of transactions that make up the block and the hash of the whole strong fall in a target space that is small in relation to the larger output space of the hash function.

Proof of stake is a consensus mechanism where we approximate in proportion to the ownership of the currency.

Tokens

- Token contracts are a special type of contract that define a bundle of conditional rights for the holder. They can represent anything from a store of value to a set of permissions in the physical, digital, and legal world. They are also used to create incentives among participants at low cost.
- Tokens offer several benefits: a) greater transparency, b) lower transaction costs, c) greater liquidity, and d) new use cases for businesses to experiment with. They are typically only a few lines of code.
- Assets are just anything that have a monetary value attached to it. Ownership is the legal right to possess it, including suage rights. But NFTs do not necessarily convey ownership over the underlying idea or product/service they represent – they are a hash that directs to an agreement.

Types of Tokens

There are a lot of ways to describe similar phenomena, but it’s useful to have a context.

- Exchange tokens – not issued or backed by any central authority, intended rather as a means of exchange
- Utility tokens – these grant holders access to product or services, but not the rights to them as investments – typically for access to a flow of consumption
- Security tokens – these grant holders the rights and obligations to an asset
- Governance tokens – these grant holders a right in the design and governance of a protocol

Guest Lecturer: Eric Allmendinger from Persona

UNIVERSITY of NICOSIA

Questions?

Contact:

Christos A. Makridis | Professor | Makridis.c@unic.ac.cy
Evgenia Kapassa | Teaching and Research Associate | kapassa.e@unic.ac.cy