Blockchain-Based Financial Tools

Subjects: Computer Science, Information Systems

Contributor: Marco Zecchini

Blockchain technology has had a close connection with finance since the beginning. It is well known that one of the main success story for blockchain is Bitcoin, the first cryptocurrency. Beside the original novelty of implementing transactions in a decentralized setting, it is now clear that blockchains enable a wide range of novel financial instruments, many of which are specific of blockchain-based economic systems.

Keywords: Internet of Things (IoT) ; blockchain

1. Guaranteed Payments and Funds Unlocking

Blockchain-enabled payments can be made arbitrarily complex. In simple cases, spending or transferring funds is allowed after proving their possession. However, in general, blockchain technologies support the adoption of a wide variety of conditions, such as the following examples:

(1)having the consent of *m* out of *n* other users (1≤m≤n);

(2)checking the expiration of a deadline;

(3)checking that some other transaction has actually occurred.

Further, any logical combination of the above is possible, and since in IoT a device can signal the occurrence of a physical event in blockchain (by a suitable transaction [1][2]), this can be part of the condition as well. For example, this enables automated escrow systems [1][2], in which funds are unlocked when an actor executes some physical action. For blockchains that support smart contracts, any user that is entitled to create a smart contract can create his/her own custom conditions. For ad hoc blockchains with no smart contract support, this flexibility is also available, but decisions regarding which kind of conditions to adopt have to be made by the system designer in advance.

Sophisticated payments between parties are used in many use-cases: in SavePlanetEarth [3], individuals exchanges SPE tokens with NFTs representing carbon credits; in MedicalChain [4], medical researchers buy access to a relevant patient's health data in a marketplace, paying in cryptos. Escrow payments are adopted in [5], where a user who is willing to rent a vehicle directly buys an unlock token from a smart contract to activate the vehicle.

2. Tokens

Tokens are digital assets whose ownership is recorded in a blockchain. Almost all unpermissioned blockchain networks have a *native* token (more properly called *coins* or *cryptocurrencies*). However, many technologies provide easy means to create new kinds of *non-native* tokens for specific purposes. Each kind of token (native or not) has specific rules according to which token units are created (*minted* or *mined*), transferred, and destroyed (*burned*). These rules are designed to fit the purpose of the token and can vary greatly among tokens. Some reasons to have custom tokens are the following:

- They can be given to a thing provider, owning a thing, as a reward for allowing other users to use that thing.
- They can be used as money to buy a service or data within the ecosystem.
- They can represent a specific real thing so that ownership of the thing is represented in blockchain by the ownership of the token. This is the case of *non-fungible tokens* (NFTs), also called *asset tokens*.
- They can be sold to investors and enthusiasts in the initial phase of a project for the purpose of raising fiat money funds by means of an Initial Coin Offer (see below). In turn, token holders get some rights within the newborn ecosystem, such as, for example, having access to an offered service at a lower price, getting a small share of the income, or expressing a vote for the governance of the project.

- They can be used as a security to represent a share of the value of the ecosystem that can be traded and exchanged on a market (see below).

The first three cases are realized by standard blockchain features, possibly integrated with capabilities of IoT devices to coordinate transactions with physical events. The last two cases require relying on exchange services, which might be completely independent of the IoT ecosystem or might be integrated with it.

In addition, approaches are possible where multiple tokens are used in a single ecosystem, where, for example, one token has the objective of representing the value of the ecosystem as a whole and is traded on the markets, and another serves as a cryptocurrency to buy and sell services in the ecosystem. The value of the second kind of token might be artificially anchored (*pegged*) to a fiat currency to keep the price of services within the ecosystem stable. This approach usually requires an oracle to observe the current exchange ratio of the first token with a fiat currency and an automatic way to transform the first kind of tokens into the second one, on demand. PlanetWatch [6] adopts two tokens with this perspective: Planet tokens are used as a mean to reward citizens for their provided measurements, and they are traded on the market; Earth Credits can be used to obtain services or products within the PlanetWatch ecosystem, and they can be exchanged either with euros, at a fixed price, or with Planet, at a price depending on its quotation. In Helium [7] and Powerledger [8], two tokens are similarly used.

It is worth mentioning that, since different sets of rules result in different “economic behavior”, the new field of study called tokenomics (heavily based on game theory; see, for example, [9][10][11][12][13]) aims at understanding and foreseeing the effect of a certain set of rules.

Further information about the wide variety of possible tokens, their purposes, and their rules can be found in several works (see, for example, [14][15]).

3. Incentives

Incentives are an important part of any unpermissioned decentralized architecture. They are usually provided as tokens that reward a positive behavior and that can be converted into something valuable (e.g., fiat money or services) for whoever expressed that behavior. In general, in a blockchain, the reward is given for processing transactions and participating in the creation of new blocks. Integrating IoT with blockchain, incentives could be provided to motivate general positive behaviors, such as keeping some device active or hosting sensors. This may be not directly linked to a certain service or object to be actually used by anyone. In fact, there is some value just in having a part of the system be available for its use. This may motivate thing providers to join a project even in the very beginning phase, when end users are unlikely to buy any service. The possibility to reward service availability with freshly created tokens is clearly a value added of the blockchain adoption, in which the token creation strategy can be decided as part of the design of the system. From an architectural point of view, the only critical point is to assess that the condition for the reward holds. Related information may either be directly obtained from smart devices or assessed by an oracle. For example, in PlanetWatch [6], citizens are rewarded when their measurements are uploaded to the blockchain, and in Helium [7], rewards are given when thing providers contribute to prove-of-coverage and to route data.

4. Exchanges and Offsetting of Exchange Rates

Exchanges allow one to buy/sell tokens, either for other tokens or for fiat currency. They are fundamental services that allow people to buy tokens to be used in an ecosystem or to convert tokens earned in an ecosystem into fiat or other cryptocurrencies. They are normally centralized, but there are examples of blockchain-based decentralized exchanges [16][17], which can possibly be integrated into user applications [18]. Certain IoT ecosystems may have among their goals the purpose to create or facilitate a market. In this case, some form of decentralized market management may be part of the ecosystem. The Power Ledger project [8] is a prominent example of this approach for smart grids. A token that is traded in an exchange varies its *price* (or *exchange rate*) over time. This feature is considered good if the token is meant to represent the value of the ecosystem, since it allows the token owners to gain if the project is successful. On the other side, if the token is meant to be used to buy services or data in an ecosystem, excessive price inflation may have a catastrophic effect, possibly making the actual price of services or data offered in the ecosystem no longer competitive. It is possible to offset the latter problem by pure technological means. In fact, by means of an oracle, it is possible to record in the blockchain the exchange rate of a token with respect to a fiat currency. Clearly, transactions on a blockchain must be performed using a token; however, using the last exchange rate, it is possible to dynamically adjust service/data prices expressed with the token so that they are stable when expressed in fiat currency. In the vehicle-renting system devised in

[5], at the time of renting, the client application exchanges money with a cryptocurrency (ETH in their case) in the background to maintain a constant rental cost. Similar approaches are realized by Helium [7] and Power Ledger [8].

5. Staking

As written above, using a blockchain, it can be possible to realize mechanisms that lock tokens and unlock them only when certain conditions hold. Imposing users to lock tokens before allowing them to do certain actions is called *staking*. Using blockchain, the realization of staking is easy. In fact, funds can be locked for a period of time, and it is enough to programmatically check the presence of the stake in blockchain before allowing the execution of the specific action. There are several reasons to adopt staking.

- A first use of staking is to guarantee that a user has correctly fulfilled a certain task. Clearly, there should be a way to assess the correct execution of the task. In the IoT world, this may encompass taking data from a device or from an oracle. If the task is executed correctly, the user can get the benefit of their work and continue their job (or stop and get staked tokens back). If the user is recognized to cheat, the user is deprived of their staked tokens. This approach is used in escrow systems and in proof-of-stake consensus algorithms. In IoT systems, for example, a user can promise to keep a device up and running and can guarantee his/her honesty by staking some tokens.
- Staking can be useful to avoid denial of service attacks and Sybil attacks [19]. In fact, an attacker can emulate a large number of users, nodes, or devices, essentially for free. In this way, the attacker can subvert certain systems (e.g., voting, blockchain consensus, or reputation systems). Forcing each user to stake some tokens makes the cost of the attack proportional to the amount of users, nodes, or devices being emulated. Note that this also impacts the IoT world, since cheap devices are usually easy to clone maliciously. On the other hand, it is possible to create hard-to-clone devices by wiring private keys and having a public key infrastructure that signs corresponding certificates. However, this approach centralizes the trust in one, or a few, certification authorities, which is undesirable in a decentralized architecture. An example of a decentralized certification approach based on blockchain is described in [20].
- For projects that are valued using the price of a token, forcing users or thing providers to stake some tokens helps to reduce the amount of tokens in circulation. The more users or thing providers want to put tokens at stake, the higher is the demand for the token, and hence, according to the law of supply and demand, the higher is the price of the token. In other words, it is possible to obtain a non-speculative growth of the value of the token (i.e., a growth that matches the growth of the user base) by carefully designing the rules and adopting the blockchain to enforce them [21]. This approach is used in non-IoT blockchain-based services (e.g., [22][23]). Clearly, this is a general approach that can be fruitfully applied also in the context of blockchain-based IoT ecosystems.

For example, Helium [7] requires providers of validator nodes to put some Helium native tokens (HNT) at stake. In this case, staking increases the price of HNT. A complex system of penalties is not applied on staking, but rather, the amount of work reward is limited.

6. Burn-and-Mint Equilibrium

This approach was pioneered by the Factom blockchain-based data integrity service [24] and has now been adopted also in the IoT context by the Helium [7] network. In this model, the tokens paid by a consumer are not earned by anyone but simply burnt. This approach decouples the amount paid for data or services from the amount of tokens earned by the thing provider. Now, suppose one fixes the price p paid by the consumer in fiat currency and charges the consumer by the amount of tokens t that corresponds to p at the current exchange rate. To do that, the architecture has to include an oracle that regularly acquires the last exchange rate of the token and provides it to the blockchain to be used to compute the amount of tokens to be charged for each payment. Let B be the amount of burnt tokens in a certain unit of time. Let M be an amount of new tokens that is periodically minted and distributed among all nodes or thing providers proportionally to the job they have done in that period [21][25][26]. Assume that M is constant, and suppose that starting from an equilibrium state in which B=M, and hence the amount of circulating tokens is constant over time. An increase in demand increases the burning rate B with respect to the constant token-minting rate M. Token scarcity makes the token price increase. In turn, a higher token price limits the demand, forcing B to stop increasing. Intuitively, the system is expected to settle into a new equilibrium at a higher price [21][25][26]. The opposite is true if demand decreases. Further, nothing prevents one from changing M artificially to achieve different objectives. A formal analysis of these kinds of blockchain-based economic systems can be found in [27].

References

1. de Camargo Silva, L.; Samaniego, M.; Deters, R. IoT and blockchain for smart locks. In Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 262–269.
2. Han, D.; Kim, H.; Jang, J. Blockchain based smart door lock system. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 18–20 October 2017; pp. 1165–1167.
3. SavePlanetEarth (SPE). Whitepaper: A Carbon Sequestration Crypto Project. Available online: https://saveplanetearth.io/SPE_WhitePaper.pdf (accessed on 30 November 2021).
4. Medicalchain. Whitepaper: Own Your Health. Available online: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf (accessed on 30 November 2021).
5. Valaštín, V.; Košt'ál, K.; Bencel, R.; Kotuliak, I. Blockchain based car-sharing platform. In Proceedings of the 2019 International Symposium ELMAR, Zadar, Croatia, 23–25 September 2019; pp. 5–8.
6. Planetwatch|Air Quality Affects Your Health. Look after the Air You Breath. Available online: https://www.planetwatch.io (accessed on 29 October 2021).
7. Helium, People-Powered Networks. 2021. Available online: https://www.helium.com/ (accessed on 30 November 2021).
8. Power Ledger Whitepaper. Available online: https://www.powerledger.io/company/power-ledger-whitepaper (accessed on 29 October 2021).
9. Tan, L. Token Economics Framework; SSRN Scholarly Paper ID 3381452; Social Science Research Network: Rochester, NY, USA, 2019.
10. Au, S.; Power, T. Tokenomics: The Crypto Shift of Blockchains, ICOs, and Tokens; Packt Publishing Ltd.: Birmingham, UK, 2018.
11. Lamberty, R.; de Waard, D.; Poddey, A. Leading Digital Socio-Economy to Efficiency: A Primer on Tokenomics. arXiv 2020, arXiv:2008.02538.
12. Liu, Z.; Luong, N.C.; Wang, W.; Niyato, D.; Wang, P.; Liang, Y.C.; Kim, D.I. A Survey on Applications of Game Theory in Blockchain. arXiv 2019, arXiv:1902.10865.
13. Kim, H.M.; Laskowski, M.; Zargham, M.; Turesson, H.; Barlin, M.; Kabanov, D. Token Economics in Real Life: Cryptocurrency and Incentives Design for Insolar's Blockchain Network. Computer 2021, 54, 70–80.
14. Oliveira, L.; Zavolokina, L.; Bauer, I.; Schwabe, G. To token or not to token: Tools for understanding blockchain tokens. In Proceedings of the International Conference of Information Systems (ICIS 2018), San Francisco, CA, USA, 12–16 December 2018.
15. Florie Mazzorana-Kremer. Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs). 2018. Available online: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en (accessed on 28 March 2022).
16. Home|Uniswap Protocol. Available online: https://uniswap.org/ (accessed on 18 January 2022).
17. Warren, W.; Bandeali, A. 0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain. 2017. Available online: https://github.com/0xProject/whitepaper (accessed on 18 January 2022).
18. 0x: Powering the Decentralized Exchange of Tokens on Ethereum. Available online: https://0x.org/ (accessed on 18 January 2022).
19. Urdaneta, G.; Pierre, G.; Steen, M.V. A Survey of DHT Security Techniques. ACM Comput. Surv. 2011, 43, 1–49.
20. Pennino, D.; Pizzonia, M.; Vitaletti, A.; Zecchini, M. Efficient Certification of Endpoint Control on Blockchain. IEEE Access 2021, 9, 133309–133334.
21. Coutinho, K.; Clark, P.; Azis, F.; Lip, N.; Hunt, J. Enabling Blockchain Scalability and Interoperability with Mobile Computing through LayerOne. X. arXiv 2021, arXiv:2110.01398.
22. Keep–Keep Network. Available online: https://keep.network/ (accessed on 18 January 2022).
23. Livepeer—Tokenholders. Available online: https://livepeer.org/tokenholders (accessed on 18 January 2022).
24. Factom|Blockchain Data Integrity. Available online: https://www.factomprotocol.org/ (accessed on 18 January 2022).
25. Samani, K. New Models for Utility Tokens—Multicoin Capital. 2018. Available online: https://multicoin.capital/2018/02/13/new-models-utility-tokens/ (accessed on 18 January 2022).

26. Khamisa, A. Token economies. In The Emerald Handbook of Blockchain for Business; Emerald Publishing Limited: Bradford, UK, 2021.
27. Häfner, S. Utility Token Design; Available at SSRN 3954773; Research at W3F Fundation: Zug, Switzerland, 2021.

Retrieved from https://encyclopedia.pub/entry/history/show/55177