Blockchain-based Planetary Level Autonomous Systems

Bina Ramamurthy, CSE Department, University at Buffalo
Kumar Madurai, ISE Department, University at Buffalo

Abstract

The advent of the internet ushered in extraordinary growth on many technological fronts, from e-commerce to social networking. But we are yet to find effective solutions to global problems such as plastic cleaning, pandemic management, and energy distribution. These problems are inherently prevalent worldwide and typically addressed by centralized authorities with numerous trust intermediaries, which incur significant overhead and inefficiencies. Moreover, the stakeholders and participants of these large systems are culturally, socially, and geographically diverse. Building a system connecting them to solve a global problem demands enormous trust. This trust is currently realized in the financial world using centralized intermediaries such as banks and clearinghouses. The release of Bitcoin in 2009 [1] changed this situation with its blockchain protocol (infrastructure) by enabling decentralized trust intermediation. Ethereum's smart contracts [2] followed up this innovation to strengthen trust through verification and validation. These two advances collectively enabled transactions among unknown participants anywhere, opening up opportunities and laying the foundation for addressing planetary level problems. This paper discusses the enabling features in realizing planetary-level autonomous systems and how blockchain technology elegantly incorporates these features.

Introduction

A planetary level problem is a problem that affects globally everyone in a community and cannot be easily solved by traditional centralized methods. The solution typically requires the collective involvement of participants at the grassroots level. The activities around the solution are effective when self-organized and can be motivated and sustained by some form of incentives and reward system. For example, consider recyclable plastic garbage as a planetary level problem for which a local club is organizing a volunteer-based cleaning day. For such systems to scale and sustain, a trusted platform for participant engagement is needed. A public blockchain infrastructure such as Ethereum [2] can provide this platform. The salient features enabling this blockchain platform are discussed next. This discussion is followed up with a representative use case.

Feature 1: Trust platform

There is a need for a common platform where the participants (workers) who clean up the plastics can join and get paid for the work. Any capable person or machine can participate in this system. A public blockchain will serve as this trusted platform for (i) participants to transact peer to peer and (ii) enable immutable recording of credible transactions on a distributed ledger for provenance.

Feature 2: Participant Identity

To transact on a blockchain, a participant needs an identity that uniquely identifies the participant, similar to an employee identity or a student identity. But there is no central authority to assign and manage this identity. Thus, a fundamental characteristic of a blockchain-based system is the self-generated participant identity based on a (256-bit) private-public key pair, SHA hashing, and Elliptic Curve Cryptography [3]. Participants generate their identity or account number by themselves using mechanisms and tools built around strong cryptographic and hashing algorithms [4]. The self-generation of identity is critical in building an open planetary level system, where participants can join and leave as they wish. In this situation, the participants are responsible for generating their identities, safeguarding their private keys, and managing their accounts, balances, keys, and other credentials. A special instrumentation called a wallet helps participant manage their accounts on a blockchain.

Feature 3: Wallet

The wallet manages the private keys, corresponding accounts, and balances. It also features operations to confirm a transaction, sign transactions digitally, choose a blockchain network, lock and unlock the wallet, recover wallet accounts from a secret key phrase, and others. The wallet can be a hardware or a software wallet. Typically, the software wallet is a browser plugin or a mobile wallet. The mobile wallet allows anybody with a smartphone to participate and transact on a blockchain. This smartphone capability significantly improves accessibility and broader participation required for the planetary level system. A wallet can maintain a set of accounts generated using a cryptographic process that uses a recovery phrase of keywords and a deterministic wallet generation algorithm [3]. These capabilities enhances the portability of the wallet to other devices and thus the flexibility for the owner to use it anywhere.

Feature 4: Smart contract

The decentralized autonomous organization (DAO) [5] representing the planetary system is realized using a smart contract(s). The smart contract is an executable code deployed on the blockchain. It differs from any traditional code in that has it has its own identity (account address) called a smart contract address, and this address can hold a value balance. Besides these, it can define data, functions, and rules to access the functions and data. The data represents the state of the DAO, and the functions represent the operations of the DAO. One can specify rules that control the state change and execution of operations. The state change and the transactions representing the function execution are automatically recorded on the blockchain's immutable ledger, thus realizing trust and integrity. Therefore, the smart contract is the decentralized digital equivalent of a traditional centralized organization but operates autonomously once deployed. Typically, the DAO is a long-running and self-governing entity, allowing diverse participation to perform a large-scale collective operation.

Feature 5: Governance

An organizer/stakeholder initially deploys the DAO smart contract(s) with funds allocated to the smart contract to run the desired autonomous system. The governance [6] of the DAO is democratized by involving the participants. Governance is implemented using another smart contract(s) that embodies the rules and policies, voting by stakeholders to pass or reject proposals, and incentivization for participation in governance. Thus, the governance feature allows participants to self-govern, incentivize contributions to the DAO, reward good behavior, and manage exceptions and also unacceptable behaviors.

Feature 6: Micropayment

Participant engagement is critical for the success of planetary-level systems. Micropayments [7] are small amounts of cryptocurrency to reward engagement, participation, and contribution in such systems. Micropayments have been an age-old practice among societies all over the world. These payments typically do not involve conventional financial institutions such as a bank. The Bitcoin blockchain changed all that by proving the feasibility of online payments among unknown peers.

With that breakthrough, the interest in micropayments has been revived, and rightly so. And here are some basic concepts about a micropayment channel,

1. It is defined by endpoints identified by sender and receiver account addresses
2. It facilitates small (micro) and frequent payments between sender(s) and receiver(s)
3. Payment values are typically less than the transaction fees charged on traditional transactions
4. Sender and receiver relationship is temporary; typically terminated after payment is settled and synchronized with the main channel

Figure 1 shows these concepts and the relationship between the on-chain main payment channel and off-chain side-channel micropayments between the two accounts. Anybody can join and leave the main channel, and any account can transact with any other account. We know that every transaction on the main channel is recorded on the blockchain. The main channel is permanent, as in Bitcoin and Ethereum's main chains.

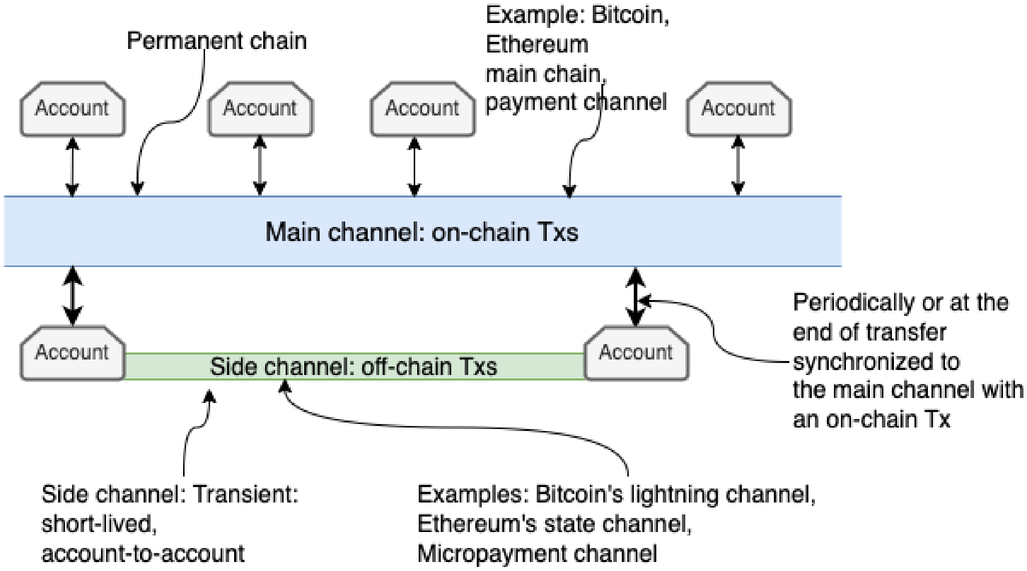
Permanent chain
Example: Bitcoin, Ethereum main chain, payment channel
Account
Account
Account
Account
Main channel: on-chain Txs
Account
Side channel: off-chain Txs
Account
Periodically or at the end of transfer synchronized to the main channel with an on-chain Tx
Side channel: Transient: short-lived, account-to-account
Examples: Bitcoin's lightning channel, Ethereum's state channel, Micropayment channel

Figure 1 Relationship between Micropayment Side Channel amd Main Chain [8]

The micropayment channel is an example of a side-channel, as shown in figure 1. It is between selected accounts, in this case, between two accounts, and is typically temporary. The transactions between the side-channel accounts are off-chain and not recorded on the chain until finally, the side-channel synchronizes with the main channel. This synchronization happens when one of the participating accounts sends a transaction on the main channel, capturing and summarizing the details of the off-chain transactions.

A Planetary level use case

To analyze a planetary level system and to apply the features discussed, we will consider a real-world problem of massive plastics cleanup (MPC) [8] on the earth. It is simply impossible for any one organization such as the United Nations to send people to clean up for all the countries in the world. So, this is a perfect decentralized problem. The MPC problem has a global scope where participants are decentralized and not necessarily known to each other. Here are some more details:

– Some verification mechanism exists to ensure the bins of plastics collected contain the right amount and the correct type of plastics. Otherwise, bins are rejected.

– A human person or robot (worker) may do this collection in bins and deposit numerous times in a day; every time the bins are verified, a message is sent to the patron organization; on receiving a message, the patron organization sends an authorized off-chain micropayment through a channel established between the organization and the worker. Potentially there may be many micropayments to the worker in a single session of plastics collection. In a given session (for example, a day), the value of a micropayment is the sum of all the previous micropayments added to the current one. Thus, a micropayment is a value monotonically increasing [8], thus accounting for the work completed, and this method prevents double-spending; in other words, cashing the same micropayment more than once.

– Instead of cashing these small payments every time a bin of plastic garbage is collected and incurring cashing fees, the worker waits until the last bin of their day and then collects the payment through one on-chain transaction (Tx). By design, this single Tx request is for the value of the final micropayment since it holds the accumulated value.

– After the payment is claimed, the channel is closed. A new channel is created, and the process is repeated for every worker and every worker session. This closing of the channel also helps in preventing double-spending. In an alternative design, the channel can be kept open between withdrawals.

The sequence diagram in figure 2 explains the operation of the MPC system. The MPC organizer deploys a smart contract (*constructor ( )* in figure 2) with a deposit funding for paying off the workers. The role of this smart contract is that of DAO. The link between organizer and a participant is established by configuring a smart contract with wallet address-identity of the worker. When a worker claims payment with the digitally signed message for an amount, the functions of the smart contract DAO verify and pay off the worker from the deposit balance in the smart contract. The micropayments sent by the organizer to a worker contain the payment value digitally signed by the organizer. The many micropayment messages (shown in figure 2) are sent through the side-channel and are not recorded on the blockchain. When the worker (with their identity and wallet) finally claims payment (*claimPayment ( )* in figure 2) using the latest digitally signed payment, the smart contract code verifies both the signer and the amount by recovering these from the signed message. The recovered pieces are hashed and compared with the digitally signed payment message. If they verify it correctly the smart contract transfers the payment to the worker's address. More technical details and a proof of the MPC concept implementation can be found in [8] along with the code for the reader to explore this use case further.

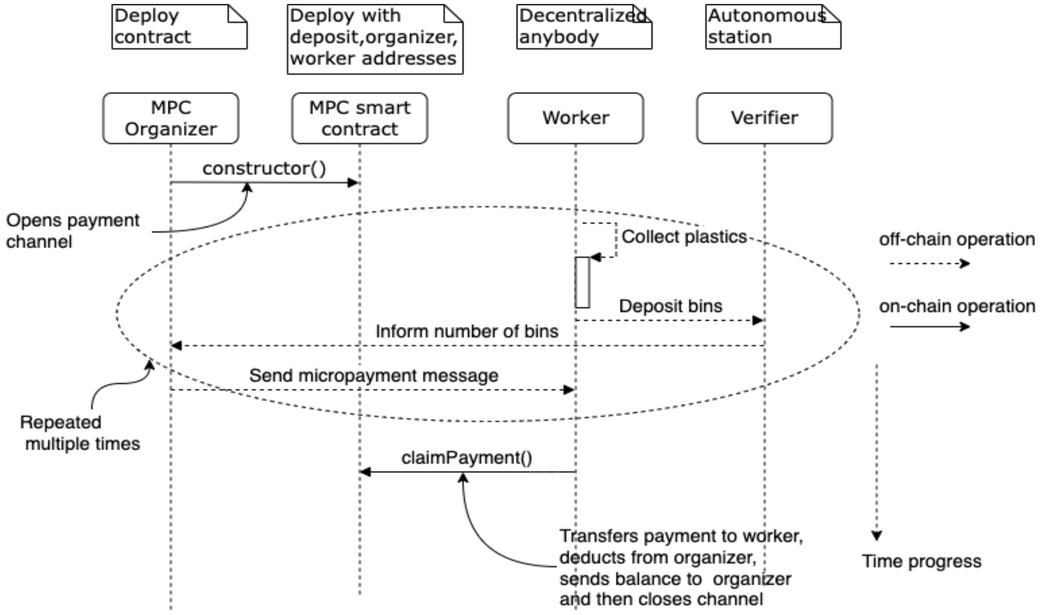

Figure 2 Sequence Diagram – Planetary Level Autonomous System MPC [8]

Summary

The paper introduced blockchain as a trusted platform for solving planetary level problems with global scope and the participation of diverse people and entities. It also discussed the unique features that power a blockchain-based solution, such as identity, wallet, smart contracts, DAO, governance, and micropayments to incentivize engagement. A use case illustrating these concepts was discussed. The model provided here for a planetary level autonomous system can be adapted to solve other planetary level problems. The paper demonstrates the enormous potential of the blockchain for solving planetary-level problems with broad impact.

References

1. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/en/bitcoin-paper, 2008.
2. V. Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/, last viewed 2022.
3. S. Nakov. Practical Cryptography for Developers. ISBN: 9786190008705, https://cryptobook.nakov.com/, MIT License, November 2018.
4. Bitcoin Improvement Protocol 39 seed phrases for private keys (BIP39), https://github.com/iancoleman/bip39, Last viewed 2022.
5. L. Liu, S. Zhou, H. Huang, Z. Zheng. From Technology to Society: An Overview of Blockchain-based DAO, arXiv:2011.14940, February 2021.
6. Y. Liu, Q. Lu, L. Zhu, H. Paik, M. Staples. A Systematic Literature Review on Blockchain Governance, arXiv:2201.07964, December 2021.
7. Solidity by Example: Micropayment Channel. https://docs.soliditylang.org/en/v0.8.12/, last viewed 2022.
8. B. Ramamurthy. Blockchain in Action. Manning Publications, https://www.manning.com/books/blockchain-in-action, 2020.