A Study on Diem Distributed Ledger Technology

G. Antonio Pierro[1,*], Roberto Tonelli[1,†]

[1]Dep. of Mathematics and Computer Science of University of Cagliari, Palazzo Delle Scienze, Via Ospedale, 72, 09124 Cagliari CA, Italy

Abstract

The paper analyzes the Diem Distributed Ledger Technology (DLT). First, the paper presents a general overview of the Diem project from a technical point of view. Second, it presents a study that aims to collect and analyze data from the Diem blockchain, in order to verify some properties declared in the technical paper. For instance, a relevant property of the Diem blockchain is its transactions' throughput, i.e. the rate at which valid transactions are committed into a block by the Diem blockchain in a one-second interval of time (transactions per seconds, TPS) and the interval of time for a transaction to be confirmed. The data were collected over a period of three months (January 1 - March 31, 2022) and made available on a GitHub repository.

The results of the data analysis show that the average transactions' throughput is about 60 TPS and the waiting time is on average 1 minute and 40 seconds. Moreover, the paper sheds light on some Diem features that are unique when compared to similar blockchains, such as Ethereum. Some of these unique features are the consensus mechanism based on the BFT consensus protocols (Byzantine Fault Tolerance, 2017), its accounting system based on a hierarchical model and its programming language, Move, used to code smart contracts. The analysis will provide a better understanding of the Diem blockchain's features.

Keywords

Blockchain, Virtual Asset Service Providers (VASPs), UTXO Model, Account Model, Move programming language

1. Introduction

During the last decade, many distributed payment systems have emerged as an alternative to centralized banking. The Diem Distributed Ledger Technology (DLT), initially called "Libra" and renamed "Diem" in December 2020, was designed and proposed by the Diem Association, a non-profit organization headquartered in Geneva, Switzerland. When Diem was introduced by Facebook in 2019, the Diem Association aimed to be a competitor in the field of payment systems, by introducing the Diem blockchain, i.e. a cryptographic payment system where each party is clearly identified and every transaction is authenticated, authorized, validated and

DLT 2022: 4th Distributed Ledger Technology Workshop, June 20, 2022, Rome, Italy

*Corresponding author.

*Corresponding author.

†These authors contributed equally.

†These authors contributed equally.

antonio.pierro@gmail.com (G. A. Pierro); roberto.tonelli@unica.it (R. Tonelli)

https://www.agile-group.org/category/persone/ (G. A. Pierro); https://www.agile-group.org/roberto-tonelli/ (R. Tonelli)

0000-0002-3805-7964 (G. A. Pierro); 0000-0002-9090-7698 (R. Tonelli)

tracked. Moreover, Libra, the Diem DLT cryptocurrency, would have the ability to maintain a stable value relative to a particular fiat currency [24]. According to the technical paper at launch, the goal was to support at least 100 validators, able to process 1000 payment transactions per second. A "validator" is the term used to describe a node of the network that helps verify and propose new blocks of transaction data [7, 17].

Diem was a blockchain payment system based on an account model with users, roles and rights, where only pre-authorised computers can access and finalize transactions. This set of pre-authorised computers participate in a consensus mechanism based on the BFT (Byzantine Fault Tolerance) consensus protocols [6, 11]. Compared to other cryptocurrencies, such as Ethereum and Bitcoin, Diem has the following features:

- The withdrawal capacity i.e. the possibility to delegate the authorization to spend to a different account.
- The Diem BFT consensus protocol, i.e. a consensus mechanism where a group of authorized validators creates, verifies, and certifies the new blocks of transactions.
- An off-chain collateral system where the underlying assets are stored with an escrow service.
- The accounting system based on a hierarchical model.
- The Move programming language is used to code smart contracts and, unlike other programming languages used to code smart contracts, it integrates resources at the type level.

The online payment market economically remains massive, which suggests enormous profit opportunities for early actors on the market. Although the WhatsApp pay attempt did not reach the expected success, Facebook came back in 2019 with Libra, then called Diem, a new project that shares similarities with the previous idea. At the same time, Facebook made it clear that it did not intend to stop at the initial 28 members, which included Paypal, Shopify, Uber, eBay, and Vodafone. They were instead planning to expand the Association to over hundred members in the upcoming years.

Table 1 shows the seven largest blockchain platforms sorted by Market Capitalization and compared to the Diem DLT. The columns of the table reports some characteristics of the blockchains, such as the presence of a stable coin and smart contract support. Stable coins are cryptocurrencies which can maintain a stable price in relation to fiat currency [5]. A smart contract is a self-executing computer program that uses the blockchain to store the contract's terms [39]. When the Diem DLT was operational, it supported a stable currency and the capability to deploy and execute smart contracts. Then, Meta, formerly of Facebook, stopped the project in January 2022.

Recently, the former Meta employees decided to continue the Diem proposal and they renamed the project to Aptos [14]. Aptos has many features in common with the blockchain Diem (https://github.com/aptos-labs). Some of these features are the possibility to deploy smart contracts written in the Move programming language and the possibility to build higher-level applications and protocols on top of the underlying Aptos blockchain. The Aptos' development network (devnet) is operational since March 2022 and it is possible to monitor their transactions via a blockchain explorer named Aptos Explorer (https://explorer.devnet.aptos.dev/) According

to the former Meta employees, the Aptos main network (mainnet) is planned to be launched in the last trimester of 2022.

Table 1
Largest blockchain platform by Market Capitalization vs Diem blockchain

	Market Cap (Billion USD)	symbol	Permissionless?	Stablecoin?	Smart Contract?
Bitcoin	771	BTC	Yes	No	No
Ethereum	362	ETH	Yes	No	Yes
Binance	65	BNB	Yes	No	No
USD Coin	50	USDC	Yes	Yes	No
Solana	35	SOL	Yes	No	Yes
Diem	-	DIEM	No	Yes	Yes

The first technical paper specified that any interests gained with the investments of the Diem Association reserve fund, which will be composed mainly of short-term government bonds will be used to cover the costs of the system, ensure low transaction fees, and pay dividends to investors who provided capital to jumpstart the ecosystem[37].

The second version of Diem DLT was introduced with an update on the technical paper in April 2020 [35]. Many popular crypto payment systems struggle to maintain a high transaction throughput with a low transaction latency. According to the technical paper, Diem attempts to solve this with the adoption of Diem Byzantine Fault Tolerance (Diem BFT) consensus protocol. Diem BFT facilitates agreement among all validator nodes on the ordering of transactions while achieving good transaction throughput and low transaction latency when scaling in the number of validator nodes. The Diem BFT fault-tolerant model remains safe when at most one-third of the nodes are faulty.

2. Background

Nowadays, there are a large number of blockchain platforms, each with its own characteristics and design decisions [1, 33]. For instance, some platforms are designed specifically to support rich and complex smart contracts (e.g., Ethereum and Solana), while others are designed to act as a bridge between digital and fiat currencies (e.g.,Tether and USDC). We list the most ten popular blockchain platforms and their characteristics vs the Diem blockchain, as depicted in Table 1.

This section describes information peculiar to the Diem blockchain such as the Move programming language 2.1 used to write smart contracts, the Proof-of-Authority (PoA) consensus algorithm and the accounting used by the Diem blockchain.

2.1. The Move Programming Language

A Smart contract is a piece of executable code that run on the blockchain to facilitate, execute, and enforce an agreement between untrustworthy parties without the involvement of a trusted third-party [23, 26]. Smart contracts have the ability to convert paper contracts into digital contracts [12, 18]. Compared to traditional contracts, smart contracts enabled users to codify their

agreements and trust relations by providing automated transactions without the supervision of a central authority [23]. In order to prevent contract tampering, smart contracts are copied to each node of the blockchain network [3, 38]. By enabling the execution of the operations by computers and services provided by blockchain platforms, human error could be reduced to avoid disputes regarding such contracts [23].

The blockchain Ethereum popularized the term by being the first public blockchain to provide a Turing complete smart contract language [41, 16]. The goal of Ethereum is to provide a world computer for which anyone can build and deploy blockchain-based applications, often referred to as Decentralized Applications (DAPPS) [27].

As well as the Ethereum blockchain, also the blockchain Diem supports smart contracts written in a different programming language which name is Move. Move is a programming language based on Rust that was created by Facebook for developing customizable transaction logic and smart contracts for the Libra digital currency. Every transaction submitted to the Libra blockchain uses a transaction script written in Move to encode its logic [4].

The key feature of Move is the ability to define customized resource types. This customized resource type supports all the operations generally available to other entities. This means the Move programming language supports passing Resource as arguments to other functions, returning them as the values from other functions, and assigning them to variables or storing them in data structures. For this reaseon Move can be defined as a language where Resources are first-class citizen.

Resources in the blockchain system are important because they provide scarcity protections: they can only ever be moved between program storage locations, never implicitly copied or deleted. The Move type system provides static enforcement of these security measures, but allows programmers to define custom resource types.

By integrating resources at the type level rather than supporting a single type of resource value (eg, Ether), the Move programming language provides programmers with the security measures they need while remaining independent of the blockchain. Any developer can define and use custom resources, without the additional re-implementation process required by ERC20 (Ethereum Request for Comment, Proposition 20) and other libraries. To protect critical resource operations from untrusted code, Move encapsulates the fields of each resource in a corresponding form. Modules are similar to smart contracts: they contain the types and procedures for creating, updating, and destroying the assets they contain. They also provide an abstraction of critical data: fields of a resource type declared within a form are protected by any other form, and operations on that resource must only be performed within its form.

2.2. Consensus Model - Proof of Authority Consensus

Consensus makes it possible for a decentralized network of computers to agree upon and share the state of the system [1]. The consensus is critical in ensuring participants can trust the transactions processed on the blockchain even when they may not trust each other [10]. Before Bitcoin, it was impossible to electronically transfer digital money without relying on a centralized authority to manage the state of the system.

Nowadays, public blockchains such as Bitcoin or Ethereum, allow anyone to participate in the consensus process as a miner. Miners compete (or effectively vote) to add new transactions

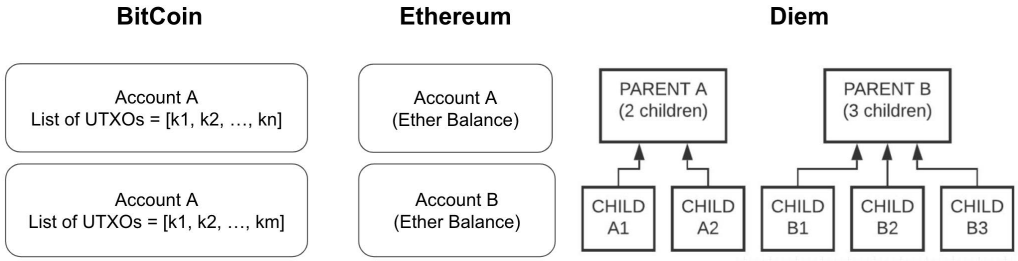


Figure 1: Address structure in different blockchains (Bitocoin, Ethereum and Diem).

to the blockchain with computing power by expending a certain amount of Central Processing Unit (CPU) cycles to solve a mathematical puzzle. This puzzle is intentionally computationally difficult to solve, yet it is very easy to verify the answer [29].

To add a block of new transactions to the blockchain, a miner must solve the puzzle. The first miner to solve the puzzle sends (proposes) the block to the rest of the network for agreement. If the network agrees on the solution to the puzzle, the miner is rewarded for creating the block and the block is added to the blockchain (the miner wins this round of competition). Through a combination of game theory and economics (effectively betting CPU cycles, which cost money, to win the reward), Proof of Work (PoW) incentivizes consensus instead of attempting to enforce it. Essentially a miner is rewarded for securing the network.

While public blockchains rely on PoW, enterprise (or permissioned) blockchains [15] tend to use the BFT consensus protocols [6]. BFT consensus is based on the idea that a pre-selected, authorized group of validators will create, verify the new blocks.

In a proof of authority consensus model, known participants leverage cryptographical digital signatures to agree upon a set of transactions and their output to advance the blockchain's state [28]. For the Diem Blockchain the set of potential entities that can participate in consensus are known as Validator Owners, while the active participants are known as the Validator Set. The adding and removing of Validator Owners and specifying the current Validator Set is left to the sole discretion of the entity managing "Diem Root" account. Validators receive transactions from clients and share them with each other through a shared mempool protocol.

2.3. Diem Accounting System

In the Diem DLT, an account represents a resource on the Blockchain that can send transactions. Each account is identified by a 16-byte hash value and there are two kinds of accounts, ParentVASP and ChildVASP accounts. The ParentVASP represents the primary account of a digital wallet, while the ChildVASP is defined as the child account of a particular ParentVASP. Multiple ChildVASPs can be created by ParentVASP accounts [20]. Figure 1 represents the address structure in different blockchains.

In Diem, a PoA will be requested from the ParentVASP, and these proofs should include all of their children's assets as well. Table 2 shows the users roles and permission supported by the Diem DLT [13].

Table 2
Diem Roles and Permissions

Role	Granted by	Unique?	Address	Has balances?	Account limits?	Fr.able?	Tx pri.
Diem Root	genesis	Globally	0xA550C18	N	-	N	3
Treasury Compliance	genesis	Globally	0xB1E55ED	N	-	N	2
Validator	Diem Root	Per Association member	-	N	-	Y	1
Validator Operator	Diem Root	At most one per Validator	-	N	-	Y	1
Designated Dealer	Treasury Compliance	N	-	Y	N	Y	1
Parent VASP	Treasury Compliance	Per VASP	-	Y	Y	Y	0
Child VASP	Parent VASP	N	-	Y	Y	Y	0

Diem uses a variant of role-based access control (RBAC) to restrict access to sensitive on-chain operations. A role is an entity with some authority in the Diem Payment Network (DPN). Every account in the DPN is created with a single, immutable role that is granted at the time the account is created. Creating an account with a particular role is a privileged operation (e.g., only an account with the ParentVASP role can create an account with the ChildVASP role). In some cases, the role is globally unique (e.g., there is only one account with the Diem Root role). In other cases, there may be many accounts with the given role (e.g., ChildVASP).

2.4. Stablecoin

Stablecoins are cryptocurrencies with the ability to maintain a stable price relative to a particular fiat currency via a "peg mechanism". A "peg" is a specified price for the rate of exchange between two assets. In the context of currencies, a peg allows foreign currencies to be traded for the chosen base currency at a fixed exchange rate. In the context of cryptocurrency, a peg refers to the specific price that a token is aiming to stay at [9].

Today, stablecoins are mostly used for trading, lending and borrowing crypto assets. They are a crucial component of the decentralized finance (DeFi) – financial services performed by applications on a permissionless blockchain [21].

Stable coins first became widely known as a potential means of global retail payments when Meta (then Facebook) announced its Libra project in 2019. Bitcoin and Ethereum rise and fall by the day and even hour, in contrast, stable coins promise to maintain their value because they are pegged to less volatile assets, like the U.S. dollar or Euro. Because of their potential use as actual currency, U.S. government officials fear the potential risks stable coins pose for consumers and financial markets if they remain unregulated. As an example, the value of the TerraUSD stablecoin (UST) crashed in the cryptocurrency market almost completely at one point on 9 May 2022 and lost its 1 USD peg to the dollar, tanking to a low of 0.02 USD [9] without giving any legal protection to their investors [22].

Stablecoins can be split into three groups according to their collateral and price stabilization mechanisms:

1. off-chain collateralized (e.g. Diem)

2. on-chain collateralized (e.g. Dai)
3. uncollateralized, purely algorithmic stablecoins (e.g. Ampleforth).

The Diem DLT was planned to be an off-chain collateralized project, i.e. it should have used use traditional reserve assets to stabilize Libra value, the Diem cryptocurrency. The Deim reserve assets should have been fiat-currency bank deposits and short-term debt, with the US dollar being the most prominent reference currency. As the reserves are not on the blockchain, a custodian is required. In order to maintain price stability, all outstanding stablecoins must be backed by reserve assets. Currently off-chain collateralized stablecoins are Tether, Binance USD and USD Coin.

Unlike the Diem DLT, on-chain collateralized projects back their stablecoins with other crypto assets. They are typically issued by DeFi applications as collateralized debt positions, i.e. a user locks in collateral and in return receives coins created by the application. Thus, the collateral is held directly in the application on the blockchain and no external custodian is needed. Currently an collateralized stable coin system is Dai [19].

Finally, uncollateralized stable coin systems try to keep prices constant by algorithmically adjusting the outstanding number of tokens according to demand. If prices are above the peg, the algorithm will distribute new coins to users, thereby eventually reducing the price. If prices fall below the peg, the system will sell a sort of bond to users in exchange for stable coins. The stable coins received will then be destroyed, leading to a price increase. If prices then move above the peg again, bondholders will be prioritized in the distribution of new coins. In theory, this system incentivizes users to buy bonds if prices fall below the peg and rewards them afterwards as prices exceed the peg again. Currently an uncollateralized stable coin system is Ampleforth [25].

Table 3 shows the blockchains that support stable coins grouped by the stabilization mechanism.

Table 3
Stable coin blockchain grouped by the stabilization mechanism

Blockchain	Crypto Coin	Market Cap (USD)	Stabilization Mechanisms	Max	Min
Diem	Libra	-	Off-Chain Collateralized	-	-
Tether	USDT		Off-Chain Collateralized	1.002	0.999
Binance	BUSD	17,706,848,087.24	Off-Chain Collateralized	1.002	0.998
Dai	DAI	8,855,233,197.17	On-Chain Collateralized	1.010	0.985
Ampleforth	AMPL	87,155,777.68	Uncollateralized	2.11	0.91

3. Research Methodology

The main aim of the study was to better understand the Diem blockchain performance, in terms of number of transactions per second and waiting times. The study presupposes that a blockchain has a better performance than another when the former has a higher number of transactions per second and shorter waiting times when compared to the latter.

Thus, the study was designed to address the following research questions (RQ):

- RQ1: Can the Diem blockchain have a better performance in terms of number of transactions per second when compared to other blockchains, such as Bitcoin and Ethereum?
- RQ2: What are the waiting times to confirm the transactions in the Diem blockchain?

To answer the research questions, the methodology of the study consists of three research phases: a) Data Collection, b) Data Modelling, and c) Data Analysis and Results. The following subsections describe each research phase.

3.1. Data Collection

The Diem DLT provides an application program interface (API) to interact with the blockchain. We developed a script that performs a POST request to the API endpoint (https://testnet.diem.com/v1), to collect the data from the Diem blockchain. The script queries the Diem API at regular intervals of 100 milliseconds and it downloads 1000 transaction payloads for each request. A timeout of 100 milliseconds is required to avoid sending too many requests in a given interval of time and receiving the "Too Many Requests" server error. Within the rate-limit of 100 milliseconds, we collected 3.500.000 transactions, which were submitted by Diem users and available on the Diem test network. The same data can also be downloaded from a block explorer, but the collection takes much more time because each request can download just the data of a single transaction. The two block explorers available to download the data transactions are the "InDiem Blockchain Explorer" (https://indiem.info/explorer) and the "Diem Blockchain Explorer" (https://diemexplorer.com/testnet).

Table 4 shows the summary of the transactions data-set.

The mean, the median, minimum (min), the 25th, 50th, and 75th percentiles and maximum (max) are calculated for each variable shown in the table. Some of these data are the size of the script used to execute the transaction computed in bytes, the gas units used to execute the transaction (gas_used), and the number of transactions added to the Diem blockchain in a one-second interval of time (TPS) [32].

The data were collected as distinct files in JSON format. Listing 1 shows an example of JSON-RPC request used to query the Diem block data. For instance, the second value of the "params" list is an integer value (max=1000) that can be used to limit the number of transactions returned. Listing 2 shows an example of JSON-RPC response used to store the Diem transaction data. The request 1 returns the transactions' information about a confirmed block in the Diem DLT.

Table 5 describes the structure and the elements of the data related to the user transaction on the Diem test network.

Listing 1 shows an example of JSON-RPC request used to query the Diem block data. For instance, the second value of the "params" list is an integer value that can be used to limit the number of transactions returned; the max value is 1000.

Listing 1: JSON-RPC request to query the Diem DLT

```
{
  // Request: fetches 10 transactions
  curl -X POST -H "Content-Type: application/json" \
  --data '{"jsonrpc":"2.0","method":"get_transactions", "params":[ 100000, 10, false ],"id":1}' \
  https://testnet.diem.com/v1
}
```

Table 4
Summaries of the transactions data-set

	file size (B)	gas_used	bytesLength	scriptBytesLength	TPS
Min.	370.0	74.00	834	526.0	0.00
1st Qu.	606.0	74.00	1066	758.0	48.00
Median	606.0	74.00	1066	758.0	60.00
Mean	605.2	77.81	1065	757.2	62.45
3rd Qu.	606.0	74.00	1066	758.0	80.00
Max.	606.0	1748.00	1066	758.0	180.00

Listing 2: Transsaction JSON Response


```
{
  "bytes": "00f942c6ed8cab022562617cb36...",
  "gas_used": 479,
  "hash": "af6611b875d2f291c575ff36d...",
  "transaction": {
    "chain_id": 3,
    "expiration_timestamp_secs": 1645710527,
    "gas_unit_price": 0,
    "max_gas_amount": 1000000,
    "public_key": "ae4ccb911d6d36248ee3aedd437...",
    "script": {
      "amount": 1,
      "arguments": [
        "{ADDRESS: 34FCA44C571B29CC0AFF63363609B325}",
        ...
      ],
      "code": "a11ceb0b0...",
      "currency": "XUS",
      "metadata": "",
      "metadata_signature": "",
      "receiver": "34fca44c571b29cc0a...",
      "type": "peer_to_peer_with_metadata"
    },
    "script_bytes": "e001a11ceb0b01...",
    "script_hash": "04ea43107fafc12adcd09...",
    "secondary_public_keys": [],
    "secondary_signature_schemes": [],
    "secondary_signatures": [],
    "secondary_signers": [],
    "sender": "f942c6ed8cab022562617cb361a1ad84",
    "sequence_number": 375,
    "signature": "3e72d6ffc1af77...",
    "signature_scheme": "Scheme::Ed25519",
    "type": "user"
  },
  "version": 1165000,
  "vm_status": { "type": "executed" }
}
```


3.2. Data Modelling

The collected data were not suitable to perform data analysis, because reading these files takes too much time. We organized the data into three .CSV files based on their transaction type. Indeed, in the Diem DLT there are three types of transactions that can be sent by different types of accounts:

- Transactions that send payments to other accounts.
- Transactions that are sent to create accounts, mint and burn Diem Coins.

Table 5
Transactions Properties

Name	Type	Description
sender	string	Hex-encoded account address of the sender
signature_scheme	string	Signature scheme used by the sender to sign the transaction
signature	string	Hex-encoded signature of the transaction signed by the sender
public_key	string	Hex-encoded public key of the transaction sender
secondary_signers	List	Hex-encoded account addresses of the secondary signers
secondary_signature_schemes	List	Signature schemes used by the secondary signers to sign this transaction
secondary_signatures	List	Hex-encoded signatures of this transaction signed by the primary signers
secondary_public_keys	List	Hex-encoded public keys of the secondary signers
sequence_number	unsigned int64	Sequence number of this transaction corresponding to sender's account
chain_id	unsigned int8	Chain ID of the Diem network. The chain ID is a property of the chain managed by the node. It is used for replay protection of transactions.
max_gas_amount	unsigned int64	Maximum amount of gas that can be spent for the transaction
gas_unit_price	unsigned int64	Maximum gas price to be paid per unit of gas
gas_currency	string	Gas price currency code
expiration_timestamp_secs	unsigned int64	The expiration time (Unix Epoch in seconds) for the transaction
script_hash	string	Hex-encoded sha3 256 hash of the script binary code bytes used in the transaction
script_bytes	string	Hex-encoded string of BCS bytes of the script. BCS (formerly "Libra Canonical Serialization" or LCS) is a serialization format developed in the context of the Diem blockchain.
script	Script	The transaction script and arguments of this transaction

- Transactions that help account recovery, key rotation, by adding currencies and other account administration tasks.

An account can send a payment to another account by submitting a transaction. If an account A wishes to send a payment to another account B, it can do so by executing a "peer_to_peer_with_metadata" transaction script. If an account A (the ParentVASP account) wishes to create another account B (a ChildVASP account), it can do so by executing a "create_child_vasp_account" transaction script with a single ParentVASP account, a user can create up to 256 ChildVASP accounts. The transaction script allows you to specify: Which currency the new account should hold, or if it should hold all known currencies. If the user wants to initialize the ChildVASP account with a specified amount of coins in a given currency. An individual can have at most one root account per Regulated VASP. Diem Networks was suppose to create a ParentVASP account via the personal authentication key abd via the "create_parent_vasp_account" transaction script. Table 6 shows the number of transactions type found in the collected dataset.

Table 6
Types of Transactions

	transaction type	occurencies
1	create_child_vasp_account	112 320
2	create_parent_vasp_account	1 230
3	peer_to_peer_with_metadata	1 180 980

3.3. Analysis and Results

The section presents the analysis of the transactions data as modelled in the previous section. The data sets are stored in a tabular format where the rows (around one million) represent the different transactions and the columns (nine) represent their characteristics. The total size of the database is 58,1 Mega-Byte and is publicly available via Zenodo [30].

For blockchain-based applications, scalability has been extensively studied since the introduction of Bitcoin [8, 42]. We scraped and analysed the data from the Diem DLT API to compute the scalability of the Diem blockchain. Unlike other blockchains, the Diem blockchain can operate in either "normal" or "recovery" mode [2]. When the Diem DLT is on "normal mode", blocks with transactions are generated and committed in sequence. The system can switch to recovery mode in case of a failing validator node or when the system is under attack. During this time, the performance of the Diem blockchain can be negatively impacted or the processing of transactions can be temporarily put to a stop.

A previous study [2] developed a simulation model to estimate how close Diem is to realizing its goals. They calculated the amount of time a user has to wait to receive confirmation that a transaction made on the blockchain will not be changed. The results showed that, for 100 validators, that amount of time is 10 seconds. As it comes to transaction throughput, the Diem blockchain still requires major improvements, as in the best case only 300 transactions per second were estimated for 100 validators.

Another study [40] have set up an infrastructure made of physical servers (14 cores with 384GB of RAM) to measure the number of transactions Libra DLT can process in a particular time span. They have shown that the Libra blockchain can process about one thousand transactions per second at most (one validator active), but the performance drops significantly as the number of validators increases (350 TPS with 16 validators). They compared their results with other permissioned blockchains and they found in particular that Diem has worse performance when compared to the Hyperledger Fabric.

Table 7 below shows the TPS and average transaction confirmation time of Diem DTL vs. other blockchains. The data about the Bitcoin and Ethereum blockchains have been taken from different academic works.

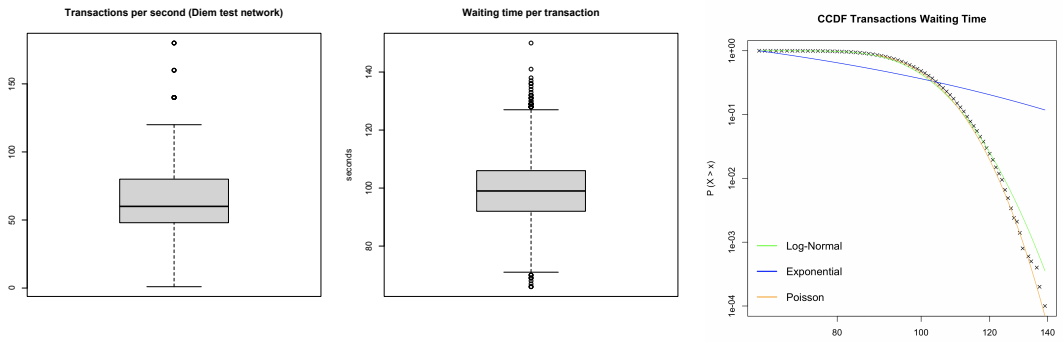
As depicted in table 7, Ethereum has a transaction speed of 15.6 transactions per second.

The rate at which valid transactions are confirmed per second in the Ethereum blockchain is higher when compared to Bitcoin. However, the TPS of Ethereum is low compared to the TPS of Diem DLT, which has over 60 transactions executed per second. Figure 2a shows the number of transactions that the Diem test network can process each second (TPS).

Figure 2c shows the power complementary cumulative distribution (CCDF) as a function of the transaction waiting times in the memory pool before being confirmed in the Diem Blockchain.

Table 7
Diem TPS Comparison against Bitcoin, Ethereum

	mean (TPS)	max	min	std
Bitcoin	4.60	-	-	-
Ethereum	15.60	-	-	-
Diem (test network)	65.51	185	0	35.72
Diem (simulation model)	80.00	300	0	-
Diem (14 cores, 384GB RAM, 16 peers)	350	-	-	-



(a) (b) (c)

Figure 2: (a) Transactions per second in the Diem test network. (b) Waiting time per transaction. (c) CCCDF of the Waiting time per transaction

The empirical CCDF seems to be well fitted by Poisson's law shown as the continuous thin orange line curving downward. Other academic studies on other blockchain suggest that the waiting time for transactions in the memory pool has a trend that follows Poisson's law [31].

4. Conclusion

Blockchain technology is rapidly evolving. Understanding the core components of the technology and how they work together is crucial to make it available also to a larger audience [43]. Each component of the blockchain system plays an important role in the technology stack. This study sheds light on some components of the Diem DLT, such as the consensus and the specificity of the Move programming language used to write smart contracts.

According to some academic sources [36, 34], the project failed for political-economical reasons. Nonetheless, some ideas of the project have been adopted and could be adopted by other blockchains. For instance, the Diem consensus allows having a better TPS when compared to other blockchains, such as Ethereum and Bitcoin. Moreover, unlike the consensus mechanism adopted by other blockchains, such as Ethereum and Bitcoin, the Diem BFT consensus protocol allows being compliant with the law in order to achieve large-scale adoption.

The data collection and analysis of the Diem transactions, even though performed on the

test network, show that the transaction throughput, expressed as a number of transactions per second, is better when compared to other popular blockchains. This is very important to achieve large-scale adoption of this technology, as it can support a larger number of transactions Another important characteristic of Diem blockchain, that has already been taken as a model by other blockchains, is the use of traditional reserve assets, such as government bonds, and stable fiat currencies, like the USD, to make the cryptocurrency value stable.

Finally, the programming language Move allows for defining custom resource types. This feature helps smart contract developers write business logic for wrapping assets and enforce access control policies without using external libraries. For all these reasons, the study can provide useful insights for any blockchain developers to choose the right components for a successful blockchain adoption at a larger scale.

Acknowledgments

This research was supported by "Fondazione di Sardegna" through the project "Analysis of innovative Blockchain technologies: Libra, Bitcoin and Ethereum" (CUP: F72F20000190007).

References

[1] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi. Certificate validation through public ledgers and blockchains. In *ITASEC*, pages 156–165, 2017.

[2] Jeanpierre Balster. Investigating the scalability of the diem blockchain: A simulation approach. *Eindhoven University of Technology Press*, 2021.

[3] Massimo Bartoletti, Letterio Galletta, and Maurizio Murgia. A true concurrent model of smart contracts executions. In *International Conference on Coordination Languages and Models*, pages 243–260. Springer, 2020.

[4] Sam Blackshear, Evan Cheng, David L Dill, Victor Gao, Ben Maurer, Todd Nowacki, Alistair Pott, Shaz Qadeer, Dario Russi Rain, Stephane Sezer, et al. Move: A language with programmable resources. *Libra Assoc.*, 2019.

[5] Dirk Bullmann, Jonas Klemm, and Andrea Pinna. In search for stability in crypto-assets: are stablecoins the solution? *ECB Occasional Paper*, 1(230), 2019.

[6] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OsDI*, volume 99, pages 173–186, 1999.

[7] Panagiotis Chatzigiannis and Konstantinos Chalkias. Proof of assets in the diem blockchain. In *International Conference on Applied Cryptography and Network Security*, pages 27–41. Springer, 2021.

[8] Anamika Chauhan, Om Prakash Malviya, Madhav Verma, and Tejinder Singh Mor. Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 122–128. IEEE, 2018.

[9] Ryan Clements. Built to fail: The inherent fragility of algorithmic stablecoins. *Wake Forest L. Rev. Online*, 11:131, 2021.

[10] Flavio Corradini, Alessandro Marcelletti, Andrea Morichetta, Andrea Polini, Barbara Re, and Francesco Tiezzi. Engineering trustable choreography-based systems using blockchain. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pages 1470–1479, 2020.

[11] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. *University of Southampton Institutional Repository*, 2018.

[12] Giuseppe Destefanis, Michele Marchesi, Marco Ortu, Roberto Tonelli, Andrea Bracciali, and Robert Hierons. Smart contracts vulnerabilities: a call for blockchain software engineering? In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pages 19–25. IEEE, 2018.

[13] LLM Eleni Katopodi et al. Blockchain market: Regulatory concerns arising from the'diem'example in the field of free competition 1. *EU and Comparative Law Issues and Challenges Series*, pages 197–216, 2021.

[14] Brandon Williams et al. Aptos. https://github.com/aptos-labs/aptos-core, 2022.

[15] Claudio Ferretti, Alberto Leporati, Luca Mariot, and Luca Nizzardo. Transferable anonymous payments via tumblebit in permissioned blockchains. In *DLT@ ITASEC*, pages 56–67, 2019.

[16] Stefano Ferretti and Gabriele D'Angelo. On the ethereum blockchain structure: A complex networks theory perspective. *Concurrency and Computation: Practice and Experience*, 32(12):e5493, 2020.

[17] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Blockchain-based database to ensure data integrity in cloud computing environments. In *ITASEC*, pages 146–155, 2017.

[18] Florian Idelberger, Guido Governatori, Régis Riveret, and Giovanni Sartor. Evaluation of logic-based smart contracts for blockchain systems. In *International symposium on rules and rule markup languages for the semantic web*, pages 167–183. Springer, 2016.

[19] Clemens Jeger, Bruno Rodrigues, Eder Scheid, and Burkhard Stiller. Analysis of stablecoins during the global covid-19 pandemic. In *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, pages 30–37. IEEE, 2020.

[20] Kim Peiter Jørgensen and Roman Beck. Universal wallets. *Business & Information Systems Engineering*, pages 1–11, 2022.

[21] Ayten Kahya, Bhaskar Krishnamachari, and Seokgu Yun. Reducing the volatility of cryptocurrencies–a survey of stablecoins. *arXiv preprint arXiv:2103.01340*, 2021.

[22] Evan Kereiakes, Marco Di Maggio Do Kwon, and Nicholas Platias. Terra money: Stability and adoption, 2019.

[23] Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, 14(5):2901–2925, 2021.

[24] Jin-Whan Kim. Analysis of blockchain ecosystem and suggestions for improvement. *Journal of information and communication convergence engineering*, 19(1):8–15, 2021.

[25] Evan Kuo, Brandon Iles, and Manny Rincon Cruz. Ampleforth: A new synthetic commodity. *Ampleforth White Paper*, 2019.

[26] Andrea Lisi, Andrea De Salve, Paolo Mori, and Laura Ricci. A smart contract based

recommender system. In *International Conference on the Economics of Grids, Clouds, Systems, and Services*, pages 29–42. Springer, 2019.

[27] Damiano Di Francesco Maesa and Paolo Mori. Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, 138:99–114, 2020.

[28] Lara Mauri, Stelvio Cimato, and Ernesto Damiani. A comparative analysis of current cryptocurrencies. In *ICISSP*, pages 127–138, 2018.

[29] Satoshi Nakamoto. Bitcoin v0. 1 released. *The Mail Archive*, 9, 2009.

[30] Pierro. Diem blockchain transactions data set, June 2022.

[31] Giuseppe Antonio Pierro, Henrique Rocha, Stéphane Ducasse, Michele Marchesi, and Roberto Tonelli. A user-oriented model for oracles' gas price prediction. *Future Generation Computer Systems*, 128:142–157, 2022.

[32] Giuseppe Antonio Pierro, Henrique Rocha, Roberto Tonelli, and Stéphane Ducasse. Are the gas prices oracle reliable? a case study using the ethgasstation. In *2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pages 1–8. IEEE, 2020.

[33] Giuseppe Antonio Pierro, Roberto Tonelli, and Michele Marchesi. An organized repository of ethereum smart contracts' source codes and metrics. *Future internet*, 12(11):197, 2020.

[34] Marc Pilkington. From libra 1.0 to libra 2.0 (diem): between programmed failure and renewed relevance for political economy. *Revue d'Economie Politique (forthcoming)*, 2022.

[35] Ivan Pupolizio. From libra to diem. the pursuit of a global private currency. *Global Jurist*, 2021.

[36] Yubin Qu, W Eric Wong, and Dongcheng Li. Empirical research for self-admitted technical debt detection in blockchain software projects. *International Journal of Performability Engineering*, 18(3), 2022.

[37] Jahja Rrustemi and Nils S Tuchschmid. Facebook's digital currency venture "diem": the new frontier... or a galaxy far, far away? *Technology innovation management review*, 10(12), 2020.

[38] Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti. Publicly verifiable proofs from blockchains. In *IACR International Workshop on Public Key Cryptography*, pages 374–401. Springer, 2019.

[39] Roberto Tonelli, Giuseppe Destefanis, Michele Marchesi, and Marco Ortu. Smart contracts software metrics: a first study. *arXiv preprint arXiv:1802.01517*, 2018.

[40] Jiashuo Zhang, Jianbo Gao, Zhenhao Wu, Wentian Yan, Qize Wo, Qingshan Li, and Zhong Chen. Performance analysis of the libra blockchain: An experimental study. In *2019 2nd International Conference on Hot Information-Centric Networking (HotICN)*, pages 77–83. IEEE, 2019.

[41] Weijie Zhao. Blockchain technology: development and prospects. *National Science Review*, 6(2):369–373, 2019.

[42] Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to scalability of blockchain: A survey. *Ieee Access*, 8:16440–16455, 2020.

[43] Mirko Zichichi, Stefano Ferretti, and Gabriele D'Angelo. A distributed ledger based infrastructure for smart transportation system and social good. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–6. IEEE, 2020.