Reltime Agnostic Layer 1 Blockchain

The future is here, more than money.

Status developed and launched:

- Layer 1, Proof of Authority Blockchain, gas free
- Web3 service ecosystem powered by smart contracts, including lending with and without collateral (P2P and P2M), P2P transfers, token minting, CBDC support, bridge, swap and joint accounts.
  iOS and Android app.
  Over 280 Integration APIs
- Reltime's platform
  - Is live in market with Real Estate platform in Europe and Fintech in Africa
  - Internal testing phase with EU Healthcare project and Swiss fintech
  - Is revenue generating

FRODE VAN DER LAAK, CO-FOUNDER, CTO AND INVENTOR

White paper version 5.0, last updated on 12 March 2025, Subject to future review and update

Table of contents

List of figures

List of abbreviations

ABAC	Attribute-based access control
AML	Anti-money laundering
B2B	Business-to-business
B2B2C	Business-to-business-to-consumer
BFP	Bona fide purchaser
CFT	Countering the financing of terrorism or combating the financing of terrorism
CSP	Credential service provider
CNIL	Commission Nationale de l'Informatique et des Libertés, the French Data Protection Agency
CRM	Customer relationship management
C/S	Client-server model or client-server architecture
DAG	Directed acyclic graph
DAO	Decentralised autonomous organisation
DLT	Distributed Ledger Technology
DPA	Data Protection Act
DPoS	Delegated Proof of Authority

eKYC	Electronic Know Your Customer
EMI	Electronic Money Institution
FG DLT	ITU-T Focus Group on Application of Distributed Ledger Technology
GDPR	General Data Protection Regulation
IAL	Identity Assurance Levels
IBFT	Istanbul Byzantine Fault Tolerant (or Tolerance)
ICO	Initial coin offering
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
RFC	Request for Comments
IoT	Internet of Things
ITU	International Telecommunication Union
ITU-T	ITU's Telecommunication Standardisation Sector
ITAS Act	Innovative Technology Arrangements and Services Act
KYC	Know Your Customer
L1	Layer-1 Blockchain
MDIA	Malta Digital Innovation Authority
MACP	Master Access Control Panel
MCBP	Mastercard Cloud-Based Payments
MTDPoS	Multi-Tenant Delegated Proof of Authority
OpenAPI	Open Application Programming Interface
P2P	Peer to peer (peer-to-peer)
PBFT	Practical Byzantine Fault Tolerance
PCI DSS	Payment Card Industry Data Security Standard
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PoA	Proof of Authority
PoS	Proof of Stake
POS	Point of Sale
PoW	Proof of Work

SDO	Standards Development, Organisation or Standards Developing Organisation
SET	Secure Electronic Transaction
TrVTs	Trust Value Technologies
UNCITRAL	United Nations Commission on International Trade Law

List of established DLT systems with a speed of <10 seconds

Cryptocurrency	**Average transaction time**	**As a private chain, consensus / sybil resistance mechanism**
Ripple	4 seconds	RPCA and Federated Byzantine Agreement (FBA)
EOS	1.5 seconds	Delegated Proof of Authority
Stellar	4 seconds	Federated Byzantine Agreement (FBA)
IOTA	1-2 minutes, theoretical confirmation time is almost instantly, 2 milliseconds	Tangle (DAG consensus)[1]
BitShares	2 seconds	Delegated Proof of Authority
Steem	3 seconds	Delegated Proof of Authority
Hedera Hashgraph	1.92 seconds	DAG [2]
NANO	1 second	Delegated Proof of Authority, Proof of Work and the DAG Network
MTDPoS, customised Reltime's PoA blockchain	<2 seconds	Multi Tenant Delegated Proof of Authority, 21 Node

[1] https://medium.com/nakamo-to/blockchain-vs-dag-technology-1a406e6c6242

[2] https://www.hedera.com

1 Introduction

One key factor influencing humanity's progress is the invention of money and the establishment of financial systems. Humans have used money in different forms for at least the last 3,000 years. Before the conceptualisation of money, a method of bartering was used to exchange values.

The bartering system had many inefficiencies that led the humans to use miniature replicas of tools and weapons as an exchange medium. Over time, the replicas became obsolete, and around 600 BC, metal coins were minted as an exchange medium. Around 1200 AD, paper currency was invented to solve the problems in handling coins for large denominations and convenience. Shifting to paper currency boosted international trade and financial institutions, and the ruling classes started buying foreign currency, creating the first currency market, eventually leading to currency wars. Throughout histonearlyconcept of currency evolved to solve the inefficiencies of its predecessor stage.

Since the rise of Bitcoin in late 2008, Satoshi Nakamoto's white paper revealed a new technology that could completely change the financial systems. Since then, Blockchain has evolved its capacity and been integrated into many applications. Immutable, transparent, Permissioned, and secure are the most mentioned features that blockchain provides. It was in 2015 that blockchain technology reached another major milestone. The Ethereum blockchain network has become famous around the world.

DeFi's conceptualised framework began operating on the Ethereum blockchain network in 2019. The initiation of the decentralised finance concept has been argued to be an aftermath of the 2008 financial crisis. It is the ecosystem of interaction between smart contracts, DeFi protocols, and dApps. Smart contracts allow the DeFi ecosystem to be structured similarly to our financial ecosystem. The concept has been , developinginitialised, and developing rapidly over the past two years. DeFi has become more recognised by our society in such a short period.

1.1 Problem statements

drawbacks. We need to address the following drawbacks to overcome the limitations in today's financial system immediately.;

1. **Accessibility:** Banking and the modern financial system are inaccessible to everyone. According to the World Bank[3] , globally, about 1.4 billion adults remain unbanked as of 2021.

2. **High transaction costs:** cent. In the current financial system, financial institutions or banks are required to act as middlemen to facilitate financial transactions. This middleman dependency comes with a transaction cost. Globally, sending remittances costs an average of 6.38 percent of the amount sent.

[3] https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf

3. **Transaction time:** Faster transfers of funds are not available for everyone. Most common fund transfer methods would require several days to complete a transaction.

The next transition of money will solve these problems in the current financial system. With Reltime, we are on a mission to solve these problems using decentralised finance powered by blockchain technology.

2 Market opportunity

With its decentralised infrastructure for processing payments, Reltime aims to become a leading full-service digital finance platform globally with one stable currency where SWIFT/IBAN is unnecessary for fiat transfer.

The global payments sector faced dramatic turbulence in the year 2020. 2019 the total global payments revenue grew to just under USD 2 trillion. Payments revenue outperformed the overall banking revenues and increased its share to under 40 per cent. However, the pandemic has influenced global financial markets, and payments revenue in the first half of 2020 reduced roughly USD 220 billion, an estimated 22 per cent compared with the statistics 2019. Market studies estimate that the global payments revenue 2020 will be USD 140 billion lower than the previous year - a decline of about 7 per cent.

The pandemic has also brought some shifts in consumer behaviourand accelerated the adoption of virtual banking. Several banks in multiple geographies have closed branches. In Australia, the top four banks have removed more than 2,000 ATM terminals and closed about 175 bank branches since June 2020.

The accelerated behaviour changes fuelled by the pandemic caused a fundamental shift in technologies such as open banking services, real-time account-to-account payment infrastructures, cryptocurrency adoption, and decentralised finance.

Investments in financial infrastructures such as instant payments have also begun to reap more significant benefits in the POS and e-commerce sectors. The behavioural shift results from customer expectations for faster transactions, convenience, and greater adoption of customer-facing finance applications, such as GrabPay in Singapore, MobilePay in Denmark and Finland or Vipps in Norway.

Consumers and businesses have opted for online bill settlements with the increasing demand for faster transactions. For example, in the United Kingdom, the average daily value of transactions processed by faster payments service rose more than 10 per cent from the last quarter of 2019 to the end of March 2020. In India, Unified Payments Interface (UPI)—the nation's local real-time payment system- offers mobile banking services, bill payments, and e-commerce links. UPI spending grew about 70 per cent over the first seven months of 2020—moreover, easing the monetary policies led to lower interest rates and margins.

Monetary authorities have also reduced benchmark rates in Europe, the United States, Brazil, India, and South Africa to reduce the impact of the pandemic-related recession. Market studies project that global interest margins will contract on average by approximately one-quarter per cent in 2020, compared with a six-basis-point reduction in 2019, shrinking payments revenues globally by roughly USD 82 billion. This paymentpayment sector gap is expected to fill newer financial instruments like open banking, decentralised finance, etc.

3 Reltime's vision

Provide a Agnostic Layer 1 Blockchain to any Vertical

A Brief History of Digital assets and Blockchain

In 2009, an anonymous person (or a group of people), operating under the alias "Satoshi Nakamoto," presented Bitcoin to the world and codified the concept of blockchain technology. Their idea was brilliant, and the underlying concept was simple: we don't need banks.

Technology has impacted our day-to-day lives in many aspects. A few decades ago, if you wanted to communicate with someone on a different continent, sending the information via mail would cost you money. But, as technology progressed, this process was made seamless. Today, you can send emails to any part of the world with close to zero expenses. However, the tremendous technological advancements, at least until 2009, have not changed how money works. Since historical times, one would need to implicitly trust third parties, such as banks, to send or receive money.

When Bitcoin was introduced to the world, it proved that we do not necessarily need banks to send value from one person to another, irrespective of their geographical location. As defined in the Bitcoin white paper, Bitcoin is a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution.

The core of Bitcoin is the revolutionary technology—blockchain. In simple terms, the blockchain is a record—a history of transactions in a system, keeping track of who did what and when. It creates an immutable ledger without the need for a single person or entity to oversee it.

In 2013, Ethereum published a white paper presenting an innovative idea that promised to make it easier for programmers to build their blockchain-based software without starting from scratch or relying on the original bitcoin software. In 2015, the company released its platform, Ethereum, for building software applications that can enforce an agreement without human intervention with the concept of "smart contracts."

Smart contracts were a gamechanger. Blockchain technology, confined to Bitcoin and finance applications, was expanded to other domains and industries with the help of smart contracts. In the later years, the world witnessed an explosion of decentralised applications, business models, and innovations in blockchain technology. Technologists, entrepreneurs, and people embraced the decentralisation movement.

And today, we are one step closer to complete independence from banking systems, with DeFi or Decentralised Finance. DeFi is a blockchain-based form of finance that does not rely on central financial intermediaries such as brokerages, exchanges, or banks to offer traditional financial instruments. Instead, it utilises smart contracts on blockchains. DeFi platforms allow people to lend or borrow funds from others, speculate on price movements on a range of assets using derivatives, trade cryptocurrencies, insure against risks, and earn interest in savings-like accounts. By October 2020, over USD 11 billion (worth in cryptocurrency) was deposited in various decentralised finance protocols, representing more than a tenfold growth in 2020. As of January 2021, approximately USD 20.5 billion was invested in DeFi.

In its different forms, technology has just begun to disrupt howother. Blockchain, DeFi are steppingstones to a decentralised and better future. It's a beautiful time to live through. And with Reltime, we are excited to participateof this revolution.

3.1 The reason behind Web3 and DeFi

The rise of Bitcoin and the tokenization. According to CoinMarketCap (2021)[4], a total market cap of over USD 1,500 billion is traded globallyworld, globally, and growth in DeFi from zero to over USD 70 billion in a DeFi project in 1.5 years.

Crypto assets have gained popularity because they are claimed to be securely stored forever. However, this brings up another problem, crypto storage is not accessible, financially, and technically, which can be explained as follows for Proof of Work projects:

- **Fee:** Asset storage has an associated fee. There are charges for users who transfer crypto assets in and out. Charges go to the miner when moving in and out of a wallet. Executing a smart contract has a price, too, according to its complexity[5]

- **Dilution:** Dilution is New coins are continuously generated, which will attract assets and dilutedilute, which is also a problem for cryptocurrency. New coins are continuously generated, which attracts assets and dilutes previously owned crypto.

With an approximate BTC calculation, that the current cryptocurrency market faces, merely holding BTC depreciates about 2.1 percent per annum. The current cryptocurrency market faces the problem of adding and preserving value for crypto assets.

[4] https://coinmarketcap.com

[5] https://medium.com/@tamas.blummer/bitcoins-storage-cost-38f17f46e782

3.2 Various types of DLT(used in fintech)

3.2.1 Consortium blockchain

Also known as a consortium blockchain, it operates under a leader or a group. Unlike a public blockchain, a consortium does not allow unauthorized access to the transactions. Unauthorised persons cannot add information to the block without the verification process. This is mainly used in the banking sector. Examples include R3, EWF, Corda, and B3i.

3.2.2 Private blockchain

A central authority controls the blockchain. It is used in database management, auditing, and financing. A private blockchain is beneficial as the transactions can be verified within a group. A single company or organization uses them. They are scalable and can resolve regulatory issues. State compliance with data privacy rules can also be carried out. The DLT varies between consensus algorithms. There are two types, proof of work (PoW) and proof of stake (PoS), also known as voting systems.

Private blockchains are further classified as mineable and non-mineable. In mineable, you can claim the ownership of new coins. In a non-minable private blockchain, the creator of cryptocurrency owns everything during the initial period.

3.2.3 Public blockchain

A public blockchain is based on proof of work (PoW); anyone can participate without permission. Anyone can download the code on their devices and start running a public node. They can easily detect the current state, validate transactions in the network, validate network transactions, and determine the succeeding blocks. Anyone can view and read the transactions on the public block explorer. People can also send transactions through these networks. If they are valid, they would be included in the blockchain. Some examples include Bitcoin, Ethereum, Monero, Litecoin, Dogecoin, and Dash.

3.2.3.1 Tangle

Tangle is ,a decentralized data architecture subdivision using the directed acyclic graph to maintain data structure and consensus protocol. Some of the unique features of tangle are quantum computation, transaction-free or microtransactions, and scalability. The tangle process aids in submitting transactions and increasing the number of results for faster time validation[1]. However, generating public addresses is part of quantum computation, which is helpful for more robust encryption algorithms and increases trust in the platform. For microtransactions, there is no transaction fee. The initiative is required to support this network, which helps submit the transactions. Besides that, the participants can use their computing power to trade.

3.2.3.2 Hashgraph

The hashgraph's focus is on fairness, cost, speed, and security, which helps structure the data to record and store transactions. The unique features of hashgraph efficiency are a fair network, visual voting, and a high translation rate. The conscious mechanism used in this subdivision is timestamped, which also helps provide a guarantee for recording and handling transactions. There is always a full copy of the hashgraph, and no node is required for that.

The network in this subdivision is not fully synthesised. This network system's use of bandwidth increases the efficiency of information transmission and transaction. Finally, this is considered the first network protocol to reduce communication, and therefore, a private environment needs to be developed using Hashgraph, which has increased the transaction rate.

3.3 Developing DeFi for micro transactions

Confidentiality and data authenticity are considered the most critical requirements of using DLT Technology. Immutable, and future alteration is impossible. At the micro-level of transactions, this technology is mainly used to detect if there has been any alteration to the original data. If the data has been altered, the hash value will change simultaneously, which is a strong advantage of using a hash function. Determination of the Hash value in advance is impossible, but a record of the predetermined hash value can be gained after creating data. Detecting the data alteration and summarizing the data helps in the innovative application of the DLT platform.[6].

Key encryption is used to encrypt and decrypt data in plain text, which is converted into ciphertext. Channels can be the internet or other public networks. Advanced encryption standards are a popular example of symmetric key cryptography. Everyday use of this example is seen in communication and online transactions, and assists in protecting the confidentiality of data. Data protection is provided when exchanging data across the public network. Therefore, a malicious attacker will not decipher long vital lengths and is a secure and reliable method for online bank transactions.

Digital signature technology is one of the benefits of using DLT. This asymmetric key clarifies the authenticity of transactions and provides the valid owner with a way to assure their digital identity. In a DLT transaction, the person must provide a digital signature. To use digital signature technology, an individual must create a pair of keys, public and private. The public key is publicly available; however, the private key must have higher security protection. A digital signature is required when sending a transaction to a third party. Then the sender has to use their private key. The public key is used to verify the digital signature and maintain a confidential transaction. If a malicious attacker tries to intercept the transaction with their private key, the system will identify unauthorized and deny the transaction. Providing security is the primary purpose of the digital signature for online transactions. Significant. Digital signatures are significant when transmitting certification for digital documentation. In addition to that, this entire process is conducted over the internet. Still, the authenticity of this process has helped the banking sector develop a public network with an unauthorized party. The use

[6] Hkma.gov.hk. (2019). [online] Available at https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf [accessed on January 20, 2019].

of distributed blanket Technology has provided an opportunity to use microtransactions in a cost-free way.

Concerning the above, distributed ledger technology has increased the opportunity for microtransactions with high-quality confidentiality, security, and privacy settings. The scope and opportunity have increased with the different types of technology. As the microtransactions include the minimum amount of money, the cost of this distribution system must be minimal or free. The entire discussion on DLT and its application has highlighted that using the tangled platform of DLT will be appropriate for the process of microtransactions. It is one of the DLT processes that have processes that have minimum power usage. Therefore, introducing this platform will increase the number of microtransaction facilities. It will provide appropriate security, privacy, and confidentiality for the microtransaction, and also, the essential asymmetric process helps maintain the transaction records. However, private and public keys will help us use the public network and preserve the individual's privacy.

Using the asymmetric key, the digital signature will be equally beneficial for microtransactions for maintaining individual details.

The distributed ledger system is one of the well-known procedures for its tamper-proof nature. It can facilitate the process of developing trust among the participants. It can build systems, build confidence, and improve the procedure. Any unauthorised attempt to change the contents in a block in the chain can cause the hash value to be changed. Links connect the blocks and can be helpful for the process of modification. DLT can ensure that the chain is not easily modified. It can break the chain and replace it with a shorter remaining chain than the original value.

3.3.1 Scalability

The distributed ledger technology is scalable enough to support regular daily traffic in the equity market. The blockchain scalability problem is growing due to its immense popularity and public consciousness of cryptocurrencies. There is a risk in the scalability that the distributed ledger technology will not keep up with the increasing demand of consumers. [7]. The largest cryptocurrencies on the market are Bitcoin and Ethereum.

These use the limited block technology's ability to process and execute the transactions. This will pose a danger to distributed ledger technology, as the size will have to be increased in response to the demand, which will undoubtedly lead to a considerable increase in the cost. [8].

The limited block size will lead to numerical instability and failure if the transaction size is increased, as each block will have to carry more data than it usually does. The distributed ledger technology is capable of supporting volume at peak times. The highest rate seen yet is 115,000,000 daily trades, or it can be said as 6,300 trades for every second for five unremitting hours. The distributed ledger technology is all about increasing the smoothness of financial

[7] https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html

[8] Barger, A., Manevich, Y., Mandler, B., Bortnikov, V., Laventman, G. and Chockler, G., 2017, May. Scalable communication middleware for permission distributed ledgers. In Proceedings of the 10th ACM International systems and Storage Conference (p. 23). ACM.

transactions. It has been seen to condense the processing time from months to days, and days to minutes. It is appropriately scalable in terms of processing speed and does not need to be improved at the moment[9].

There is a risk that the efficient calculations of transactions may be compromised in achieving the required speed. All the companies involved in distributed ledger technology are trying to create a market for their technology and increase their monetary profit. The main focus, however, should be on improving the stability and trustworthiness of the technology. The organisations are just demonstrating the speed of the technology, and the numbers easily pique interest without addressing the security or stability of the computations and transactions. The fact that it has performed many contracts using this technology. However, this is never independently proven or verified, yet consumers buy into this technology without confirming how it functions and performs.[10].

3.4 Conclusions

So far, the study has concluded about fintech and the distributed nature of DLT. As new technological advances are made, the sector. Fintech organisations have seen a rise in investment due to better consumer interaction. Many individuals readily use computer systems and applications to review, then, or make a transaction of their assets. The function is simple and has significantly upgraded the banking service. The DLT is a futuristic technology being evaluated by the financial industries for its uses. DLT can be a massive innovation in the financial sector, but it also comes with limitations. Experts have argued about its application and the role it provides. Governments in different countries have different rules and policies for asset transactions. DLT is yet to be evaluated by the jurisdiction for its application being safe for the individual.

Some key characteristics would be elasticity, scalability, transparency, and resource sharing. The study then evaluated the opinion about the cryptographic hash functions, which are the function that takes an input and returns a fixed-size alphanumeric string. They are used in various applications to provide improved security and authentication. Overall, the study has defined the merits and limitations of certain functions. The expert review has helped to understand the practical uses of DLT and others, even though it is an emerging technology with significant advantages over the current arrangement.

The findings around requirements between Payment methods such as Visa, Mastercard, and Amex, and DLT technology have not been extensively studied.

[9] Yamada, Y. and Nakajima, T., 2018, October. Experiments of Distributed Ledger Technologies Based on Global Clock Mechanisms. In International Symposium on Intelligent and Distributed Computing (pp. 436-445). Springer, Cham.

[10] Westerlund, M. and Kratzke, N., 2018, July. Towards Distributed Clouds: A review about the evolution of centralised cloud computing, distributed ledger technologies, and a foresight on unifying opportunities and security implications. In 2018 International Conference on High Performance Computing & Simulation (HPCS) (pp. 655-663). IEEE.

4 Reltime layer 1

4.1 Proof of Authority (PoA)

Reltime has its own Level 1, PoA blockchain, which has been running on AWS without downtime since November 2021. In 2024, it was migrated to Microsoft Azure without any downtime. Reltime is and will remain cloud agnostic. Reltime's Proof of Authority (PoA) is an algorithm with blockchains that deliver comparatively fast transactions through a consensus mechanism based on identity as a stake.

In PoA-based networks, transactions and blocks are validated by approved accounts, known as validators. Validators run software that allows them to put transactions in blocks. The process is automated and does not require validators to monitor their computers constantly. However, it requires uncompromising compromise of the computer (the authority node).

With PoA, individuals earn the right to become validators, so they are incentivized to retain the position they have gained. By attaching a reputation to identity, validators are incentivised to uphold the transaction process, as they do not wish to have their identities attached to a negative reputation. This is considered more robust than PoS (proof-of-stake). While a stake between two parties may be even, PoS does not consider each party's total holdings. This means that incentives can be unbalanced. On the other hand, PoA only allows non-consecutive block approval from any one validator, meaning that the risk of severe damage is centralised to the authority node.

4.2 Permissioned blockchain

Reltime has developed its permissioned blockchain. In contrast, permissioned blockchains are closed networks in which previously designated parties, sometimes consortium members, interact and participate in consensus and data validation. They are partially decentralised in the sense of being distributed across known participants rather than unknown participants, as in permissionless blockchains. Tokens and digital assets are possible but less common than in permissionless.

4.2.1 Pros of permissioned blockchain

Being closed to outsiders gives permissioned blockchains clear advantages:

- Decentralisation can be incremental, which allows multiple businesses to participate without all the risks of highly centralised models
- Strong privacy, because permission is needed to access transaction information
- Customisability for specific uses, because it allows diverse configurations, modular components, and hybrid integrations
- Performance and scalability because fewer nodes manage transaction verification and consensus

4.3 Consensus algorithm

Reltime aims to redefine the state-of-the-art Blockchain technology used in tenant and microtransactions. Reltime's PoA MTDPoS consensus algorithm will provide an open, scalable, fast, decentralized public ledger. The protocol is about leveraging the structural properties and potentially solving blockchain's orphan rate problem.

The ability of MTDPoS to withstand this problem and thus improve scalability is contingent on the additional rules implemented to deal with transaction consistency and any other design choices.

The Multi-Tenancy protocol built into the protocol will technically be easy to mass-adopt based on building blocks. Still, to be an accepted industry protocol, it should be able to support industry standards, such as Mastercard MCBP.

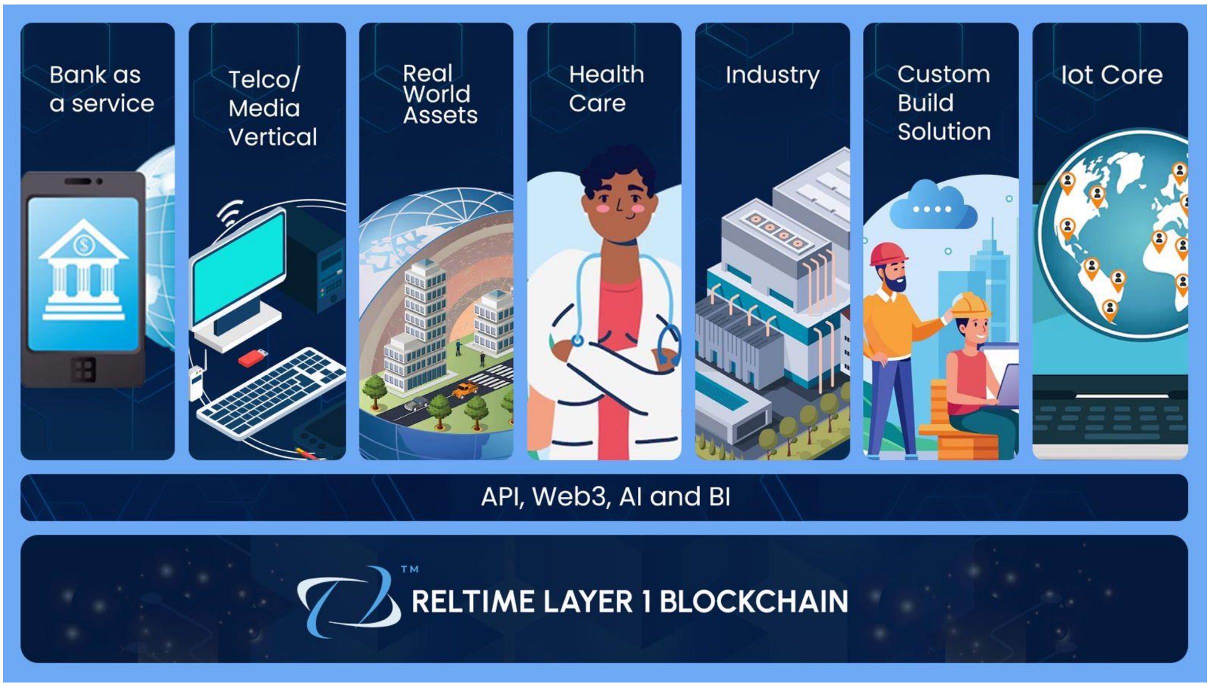


Figure 1: Overview of Reltime's Sector-Agnostic service offering

4.4 Remote payments

4.4.1 Digital wallets[11]

A mobile or a digital wallet is an application that stores your information and can carry out every type of payment. All it requires is setting up an account and linking your account or card details. You have to authenticate your identity during every payment by entering a passcode, a one-time password, or scanning your fingerprint. You can select any verification that is suitable for you.

[11] https://en.wikipedia.org/wiki/Digital_wallet

Internet payments

This mode of payment requires the sender to enter their card details on an app or website while making a payment. After entering your card details manually, or save them for future use. Another way of internet payment is when your bank account is automatically charged after payment.

Pros

- An instant way of making a payment
- Allows the user to delete card info after completion of payment

Cons

- The Website or app you are entering your details into will not always be secure, and your sensitive data might be visible to them.

4.5 Direct carrier billing

This mode allows you to pay through your mobile network carrier instead of directly, or the bank or card, which will charge you. You must enter your mobile number on the payment page, and the amount will be added to your monthly bill or deducted from your balance if you are a prepaid user. Once you have added your mobile number, you must authenticate it by verifying an OTP (one-time password).

4.6 Types of mobile payments

There are three main types of mobile payments: point of sale solutions (POS), in-store, and remote payments. These categories are further divided into subcategories.

- Point of Sale (POS) solutions.
- Near-field communication (NFC) payments.
- Near Field Communication is a wireless data for mobile devices, laptops, and other devices. NFC payment is acontactless payment method via mobile wallets. NFC payments are easy, straightforward, and convenient as they offer three safe and secure payment options. Peer-to-peer mode is where a connection can be established between compatible devices to share any data. The read or write mode allows a mobile to gather data from a device itself without reading. Card emulation is where NFC allows you to use your smartphone as a contactless credit card.

It supports all kinds of payments that a person wishes, such as money transfers, online shopping, and fees.

Pros

Hassle-free and convenient to use.
It is the most preferred mode of mobile payment.
It is very safe and secure.

Cons

It requires the retailer to have NFC reading technology.

Sound-based mobile payments
Sound-based mobile payments involve communicating very small bits of information between devices close to each other. Although the mode of payment is contactless, it requires both the sender and receiver to be within a close radius. The sender emits sound waves that are picked up by the receiver, and the payment mode is complete.

Pros
It only requires the sender and receiver to have a single software.

Cons
Security is considered an issue here because sensitive data is transmitted through sound that can be picked up by other devices in the same radius.
It may not work in a boisterous environment.

4.7 Architecture of Reltime

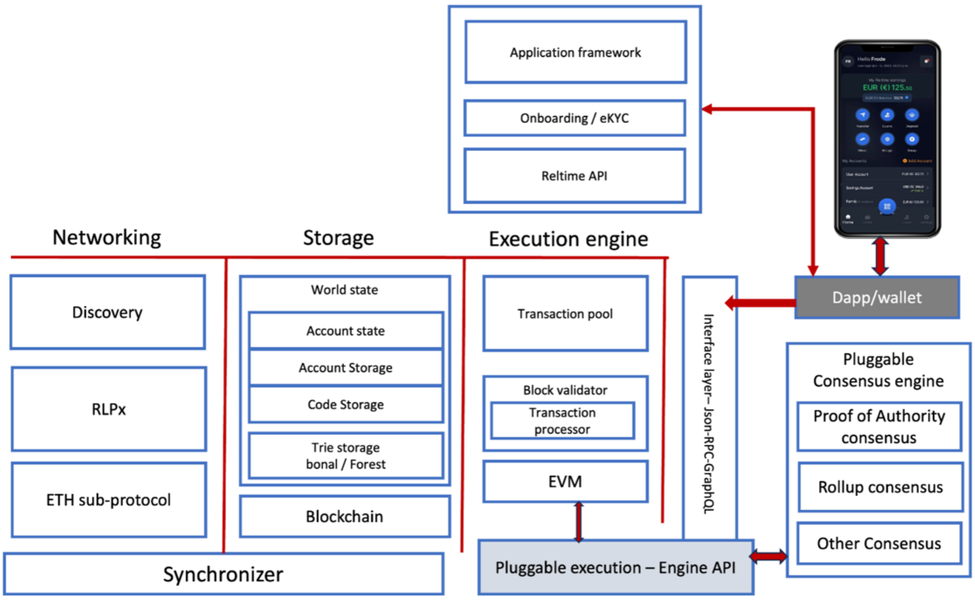


Figure 2: Overview of the platform

Reltime uses sophisticated DLT to deliver a global DeFi payments ecosystem for B2B and B2B2C. Reltime aims to reconstruct the banking system as a de facto decentralised platform that is automatic and compliant with regulations.

Below is a list of core services offered by Reltime:

Instant payments: Users can send and receive P2P payments globally with instant free money transfers through secure payments stamped in the blockchain network.

Spending insights: Users can instantly access an overview of their finances, categorised into spending, savings, and loans.

Instant lending: Users can seamlessly lend or borrow money from Reltime's P2P lending platform. Lenders can earn interest, and borrowers can take out quick loans.

Zero transaction fees: All global wallet-to-wallet transfers of Digital currency are free and instant. Reltime uses proof-of-stake-based blockchain technology to facilitate transactions.

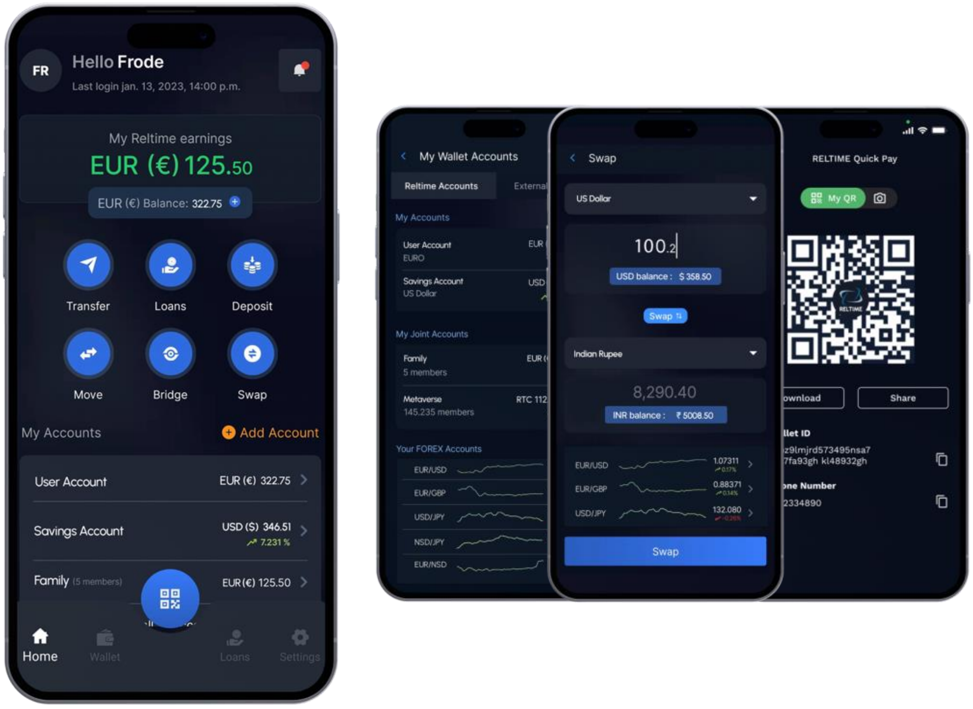
Payment cards: Reltime offers virtual, biometric, and physical payment cards issued within seconds in the look and feel of your favourite brand. Payment card subscriptions are bundled with services that matter to the user.

Joint account: Users can create joint accounts with anyone on Reltime's platform. Linking accounts enables users to share accounts for instant and free global money transfers.

OpenAPIs: Reltime provides the order to develop applications that can be integrated into the Reltime ecosystem and partner APIs that allow partners to use Reltime's services and APIs.

4.8 SuperApp, one example of the services

This is a SuperApp provided as a service for B2B and B2B2C companies, see video here [12]



[12] https://www.dropbox.com/scl/fi/33tk9es0soh99gton0aeo/Superapp-video-2.mp4?rlkey=xdlhyaghdo8uswiak2jfkvvzu&dl=0

4.9 Why Reltime?

With the DeFi infrastructure, Reltime combines the best features of fiat and crypto transactions.

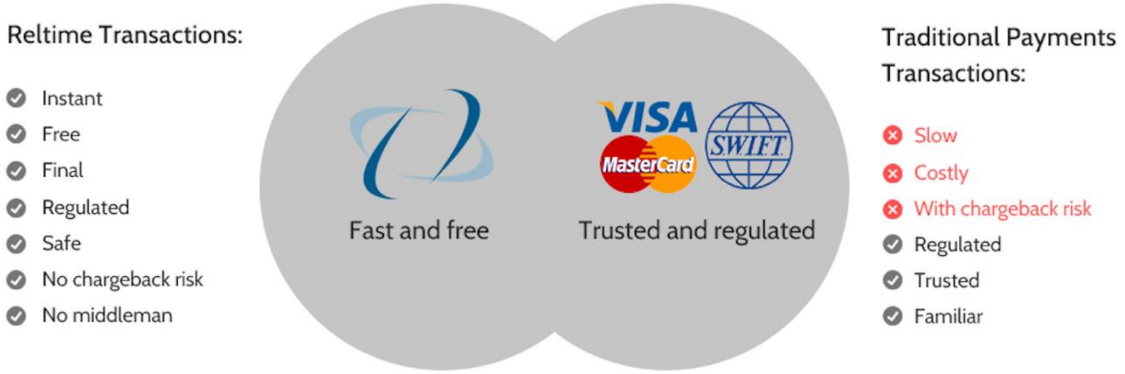


Figure 3: Overview of USPs

4.9.1 Fully automated:

Reltime has implemented a fully automated smart contracts system to eliminate costly and inefficient manual onboarding and service processes. This automation ensures a seamless, secure, and transparent user process, reducing human intervention, operational delays, and administrative costs. Key Features of Automation are:

Smart Contract-Driven Onboarding

- The onboarding process for users, businesses, and service providers is managed through self-executing smart contracts.
- Users submit necessary credentials (e.g., identity verification, KYC documents) directly into the system, and smart contracts validate the data using predefined rules.
- Any discrepancies trigger an automated workflow for further validation or rejection without manual intervention.

Decentralized Identity Verification

- Reltime integrates blockchain-based digital identity solutions to authenticate users in a decentralized manner.
- Smart contracts securely verify and store identity credentials, reducing third-party verification agencies' dependency.
- This prevents fraud, streamlines access control, and enhances security.

Automated Service Execution

- Service requests, approvals, and provisioning are handled automatically via smart contracts.

- Predefined triggers execute specific functions such as payment processing, service activation, and compliance checks without manual approval.
- This eliminates delays caused by traditional paper-based or centralized processing systems.

Cost and Time Efficiency

- By replacing manual processes with intelligent contract automation, operational costs related to administrative overhead, labor, and third-party services are significantly reduced.
- Service delivery is expedited, ensuring real-time execution with minimal errors.
- Users experience a frictionless process, improving satisfaction and engagement.

Fraud Prevention and Security

- All transactions and onboarding procedures are recorded on an immutable blockchain ledger, ensuring transparency and auditability.
- Smart contracts enforce business logic and compliance rules, reducing the risk of fraud, human errors, and manipulation.
- The decentralized nature of smart contracts enhances security and trust among users.

Scalability and Global Accessibility

- The automated system supports scalable operations, allowing Reltime to onboard and manage large user bases without manual intervention.
- Cross-border transactions and services can be executed seamlessly without intermediaries.
- Smart contracts ensure compliance with local regulations while maintaining efficiency.

4.9.2 Multi-tenant operations: Multi-tenant operations refer to a system architecture where multiple users, organizations, or entities (tenants) share the same infrastructure, resources, and application instance while maintaining data isolation and security. This approach is widely used in cloud computing, SaaS (Software as a Service) applications, and enterprise IT environments to optimize cost, scalability, and management efficiency. Key Characteristics of Multi-Tenant Operations

Shared Infrastructure with Logical Isolation

  - A single instance of the application serves multiple tenants.
  - Each tenant has its own logically separated data and configurations.
  - Common resources such as databases, computing power, and networking are shared among all tenants.

Scalability & Resource Efficiency

  - Efficient use of cloud and server resources by distributing workloads among tenants.
  - Automatic scaling based on demand without the need for dedicated infrastructure per tenant.
  - Cost savings due to shared hardware, storage, and maintenance.

Customizability for Each Tenant

- Tenants can have customized configurations, settings, and permissions.
- Support for tenant-specific branding, access control, and feature toggles without affecting other tenants.
- Each tenant can have its own user roles and security policies.

Security and Data Privacy

- Strong data partitioning to prevent cross-tenant access.
- Role-based access control (RBAC) to manage user permissions.
- Compliance with security standards such as GDPR, HIPAA, and ISO 27001 to protect sensitive tenant data.

Centralized Management and Maintenance

- Software updates, patches, and security fixes are applied centrally, ensuring all tenants benefit simultaneously.
- A single point of administration reduces the complexity of managing multiple deployments.
- Monitoring and logging mechanisms track tenant activities for improved system performance and security.

4.9.3 On-net transactions

On-net transactions refer to financial transactions within the same network or platform, meaning both the sender and the recipient are part of the same ecosystem. These transactions do not require external intermediaries, such as banks or third-party payment processors, resulting in zero internal costs, instant settlements, and enhanced security. Key Benefits of On-Net Transactions:

Zero Internal Costs

- Since transactions occur within the same network, no external processing fees exist.
- Eliminates reliance on costly third-party payment gateways or banks.
- Encourages seamless transactions for users without worrying about hidden charges.

Instant Transactions

- Payments are processed in real-time, without delays caused by interbank settlement systems.
- No dependency on traditional financial institutions, reducing transfer times from hours or days to mere seconds.

Enhanced Security & Trust

- Transactions remain within the platform’s secured infrastructure, reducing risks of fraud and cyber threats.
- Smart contracts and blockchain-based mechanisms can enhance security by ensuring tamper-proof records.

Frictionless User Experience

- Users experience seamless and instant payments without waiting for external entities' confirmation.

- Ideal for businesses, merchants, and individuals who need fast and reliable financial transactions.

Scalability & Network Effects

- As more users join the network, the value of on-net transactions grows exponentially.
- Large-scale user adoption leads to a self-sustaining ecosystem where most transactions occur internally at no cost.
- Encourages merchant adoption and financial inclusion, especially in digital economies.

Cross-Industry Applications

- E-commerce: Instant payments between customers and merchants.
- Financial Services: Secure salary disbursements and peer-to-peer transfers.
- Telecommunications & IoT: On-net billing for services without transaction fees.

4.9.4 Reltime's money transfer

Reltime enables users to send and/or receive money via peer-to-peer local and global money transfers backed by the instant minting on digital currency[13]. This enables people to bypass the challenges and pain points associated with current methods for money transfer. Reltime aims to solve three main challenges in traditional money transfer systems.

- High transaction costs.
- Slower transactions.
- Limited accessibility.

In most developing countries, many citizens, especially migrant workers, do not have access to banking facilities. They rely on unbanked services known as money transfer operators (MTO) to receive remittances. But with MTOs, the recipients have to pay a significant amount as a transaction fee out of the hard-earned money sent by the migrants.

People who have access to banking facilities receive remittances as demand drafts and bank cheques. However, it takes 2-3 weeks for a cheque to be accepted. The transaction flow of remittance starts by converting the migrant's money into USD and transferring it to the recipient's account. The amount in USD is then converted back to the recipient's local currency. Multiple currency conversions also have associated conversion charges.

Using Reltime's money transfer, users can seamlessly transfer money from one account to another in a matter of minutes with minimal transaction fees. A digital currency backs the transaction. For example, suppose a sender in USA wants to transfer money from his or her account to a recipient in India. In that case, the sender can buy digital currency from the Reltime mobile application and transfer them to the recipient's wallet. The recipient can convert the received digital currency to his/her local currency. He/She can complete the whole transaction in a matter of minutes with a nominal transaction fee.

[13] https://azuremarketplace.microsoft.com/en-us/marketplace/apps/ae8a0ba1-fc8b-4ecc-8599-0fed00daef08.offer_id-07?tab=Overview

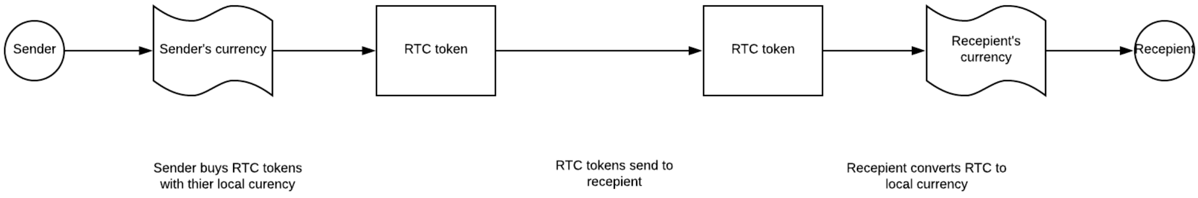

Sender
Sender's currency
RTC token
RTC token
Recepient's currency
Recepient
Sender buys RTC tokens with thier local curency
RTC tokens send to recepient
Recepient converts RTC to local currency

Figure 4: Reltime's instant money transfer

4.10 Reltime lending

Reltime lending is a P2P lending mechanism that enables users of Reltime application to avail of loans from other users. Instant loans powered by crypto instruments provide short-term liquidity for the users. Here, the users can borrow money from other users by providing collateral in fiat or cryptocurrencies. The submitted collateral would be locked in until the borrower pays back the borrowed value and the interest to the lender. Reltime allows the lenders to list digital currency they own in the platform and receive interest from borrowers.

In Reltime's application, users will be able to login into the platform by connecting their crypto wallet. If users want to lend money to others, they can list their assets in the lending portal and set details for collaterals and interest rates. If the user wants to borrow money from others, they can provide a certain guarantee fee as collateral into an escrow account.

There will be a valuation process after the lending and borrowing of the assets. Borrowers can gain profit when the valuation goes above the interest rate. The amount will below. It will automatically be reserved from the borrower's escrow account whenever the valuation exceeds the interest rate. If the valuation goes below 80 per cent of the escrow, the lender will get 80 per cent of the loan and the interest rate. At the same time, the borrower will lose 80 per cent of the guarantee fee.

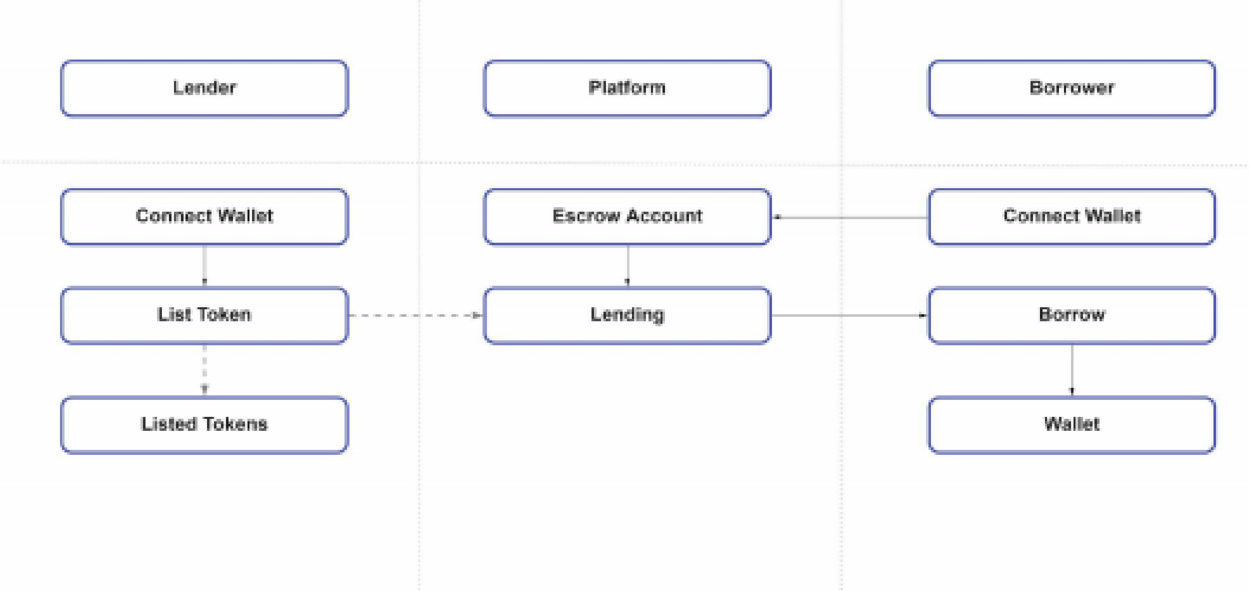


Figure 5: Overview of Reltime's lending

5 Layers of Reltime's technology

Reltime has built a global, open, permissioned, interlocking, Web3 ecosystem. Reltime is built on its own Proof-of-Authority (PoA), Layer-1 blockchain, which is accessible to individuals, businesses, and developers without any middlemen, such as conventional banks, involved.

The individual can invite other users instantly and securely, based on biometric technologies, facilitating a more secure financial instrument for everyone.

If you've researched cryptocurrencies or blockchain, you've probably encountered terms like layer one and layer two protocols.

Blockchain technology is a one-of-a-kind mix of several current technologies—cryptography, game theory, and so on—with a wide range of possible. Encoding and decoding data is a mathematical and computational discipline known as cryptography. The study of the mathematical models of strategic interaction among rational decision-makers is known as game theory. Blockchain eliminates intermediaries, lowers costs and improves efficiency by bringing transparency and security.

Without the oversight of a central authority, DLT keeps information verified by cryptography among a group of users who have agreed through a predetermined network protocol. Combining these technologies fosters trust between people or parties who would otherwise have no motive to do so. They make it possible for blockchain networks to securely exchange value and data between users.

Due to the lack of a centralised authority, blockchains must be very safe. They must also be scalability requirement, exceptionally highly scalable to handle increasing users, transactions, and other data. Layers were born out of the need for scalability concurrent to preserving top-notch security.

5.1 What is blockchain scalability?

The phrase "scaling" in blockchain technology refers to an increase in the system throughput rate measured in transactions per second. With the widespread adoption of cryptocurrencies in everyday life, blockchain layers are now required to improve network security, recordkeeping and other functions.
The number of transactions a system handles per second is called "throughput." While Visa's VisaNet electronic payment network can process over 20,000 transactions per second, Bitcoin's main chain cannot handle more than seven transactions per second.

The blockchain is the first layer in a decentralized ecosystem. Layer two is a third-party integration used in conjunction with layer one to enhance the number of nodes and, as a result, system throughput.

Blockchain developers are attempting to broaden the scope of blockchain management as Bitcoin becomes a more significant force in the commercial world. By developing blockchain layers and optimising layer two scalability, they hope to reduce processing times and increase TPS.

5.2 Hardware infrastructure layer

The blockchain's content is stored on a server in a data centre somewhere on this lovely globe. Clients request content or data from application servers while browsing the web or utilizing any apps, which is known as the client-server architecture.

Clients can now connect with peer clients and share data. A peer-to-peer (P2P) network is a large group of computers that share data. Blockchain is a peer-to-peer network of computers that computes, validates and records transactions in an orderly manner in a shared ledger. As a result, a distributed database is created, storing all data, transactions and other pertinent data. A node is a computer in a P2P network.

5.2.1 Data layer

A blockchain's data structure is a linked list of blocks in which transactions are ordered. The data structure of the blockchain consists of two fundamental elements: pointers and a linked list. A linked list list of lists of chained blocks with data and pointers to the previous block.

Pointers are variables that refer to the position of another variable, and a linked list is a list of chained blocks with data and pointers to the previous block. The Merkle tree is a binary tree of hashes. Each block contains the root hash of the Merkle tree and information like the preceding and current difficulty goal.

A Merkle tree provides security, integrity, and irrefutability for blockchain systems. The blockchain system is built on Merkle trees, cryptography, and consensus algorithms. Because it is the first block in the chain, the genesis block, i.e., the first block, does not contain the pointer.
Transactions are digitally signed to protect the security and integrity of the data contained in blockchain. A private key is used to sign transactions, and anyone with the public key may verify the signer. The digital signature detects information manipulation. Because the encrypted data is also signed, digital signatures ensure unity. As a result, any manipulation will render the signature invalid.

The data cannot be discovered because it is encrypted. Even if it is caught, it cannot be tampered with again. A digital signature also protects the sender's or owner's identity. As a result, a signature is legally linked to its owner and cannot be disregarded.

5.2.2 Network layer

The network layer, called the P2P layer, is responsible for inter-node communication. It handles discovery, transactions, and block propagation. The propagation layer is another name for this layer.

This P2P layer ensures that nodes can find one another and interact, disseminate, and synchronise to keep the blockchain network in a legitimate state. A P2P network is a computer network in which nodes are distributed and share the workload to achieve a common purpose. Nodes carry out the blockchain's transactions.

5.2.3 Consensus layer

The consensus layer is essential for blockchain platforms to exist. It is the most necessary and critical layer in any blockchain, whether it is Ethereum, Hyperledger, or another. The consensus layer is in charge of validating the blocks, ordering them, and guaranteeing that everyone agrees.

5.2.4 Application layer

The application layer comprises smart contracts, chaincode, and decentralized applications (dApps). The application layer protocols are subdivided into the application and the execution layers. The application layer comprises the programs end-users utilise to communicate with the blockchain network. Scripts, application programming interfaces (APIs), user interfaces and frameworks all part of it.

The blockchain network serves as the back-end technology for these applications, which communicate with it via APIs. Smart contracts, underlying rules, and chain code are all part of the execution layer.

Although a transaction moves from the application to the execution layer, it is validated and executed at the semantic layer. Applications give instructions to the execution layer, which performs transactions and ensures the blockchain’s deterministic nature.

5.3 Blockchain layers explained

5.3.1 Layer zero

Blockchain layer zero is made up of components that help to make blockchain a reality. The technology allows Bitcoin, Ethereum, and other Layer 1 blockchain networks to function. Layer zero components include the Internet, hardware, and connections, enabling Layer 1 to run smoothly.

5.3.2 Layer one

This is the foundation layer, and its security is based on its immutability. When people say Ethereum, they allude to the Ethereum network, or layer one. This layer controls consensus processes, programming languages, block time, dispute resolution, and the rules and parameters that maintain a blockchain network's basic functionality. It is also known as the implementation layer. Bitcoin is an example of a layer one blockchain.

5.3.3 Layer two

The overlapping networks that sit on top of the base layer are known as L2 solutions. Protocols use layer two to increase scalability by removing some interactions from the base layer. As a result, smart contracts on the primary blockchain protocol only deal with deposits and withdrawals and ensure that off-chain transactions follow the regulations.

So, what is the difference between layer one and layer two blockchain? The blockchain is the first layer in a decentralized ecosystem. Layer two is a third-party integration used in conjunction with layer one to enhance the number of nodes and, as a result, system throughput. Many layer two blockchain technologies are being implemented at present.

5.3.4 Layer two scaling solutions

Layer two protocols have exploded in popularity in recent years, and they're proving to be the most effective approach to solving scaling issues in PoW networks. The sections below explain various layer two scaling solutions.

5.3.5 Layer three

The application layer is often referred to as layer three or L3. The L3 projects act as a user interface while masking the technical aspects of the communication channel. L3 applications give blockchains their real-world applicability, as explained in the layered structure of the blockchain architecture.

5.3.6 The bottom line

One of the reasons why crypto mainstream adoption is now impossible in the blockchain business is scalability. As the demand for cryptocurrencies grows, so will the pressure to expand blockchain protocols. Because both blockchain levels have their restrictions, the eventual solution will be to develop a system that can solve the scalability trilemma.

Layer one is critical since it is the foundation for decentralized systems. Unsurprisingly, these systems aren't performing as well as we'd want. Layer two protocols to address the underlying blockchain's scalability issues. Unfortunately, most layer three protocols (dApps) currently run only on layer one, bypassing layer two. It is no surprise that these systems aren't performing as well as we'd want them to.

Layer three applications are essential because they help develop real-world use cases for blockchains. However, in contrast to legacy networks, they will not capture nearly as much value as their foundation blockchain.

6 Reltime's embedded finance

Reltime's embedded finance is an ecosystem of applications, API services, and infrastructure that facilitates the development of finance-domain products in DeFi. On a high level, Reltime Embedded Finance consists of five components: core services, marketplace APIs, partner APIs, full partner tenant, and technology layer.

6.1 Core services

The core services of Reltime's embedded finance offer white-labelled solutions for mobile wallet and payment card services, physical and virtual payment cards, payment solutions, lending solutions, a marketplace platform, personal finance, sub-accounts, and savings.

6.2 Marketplace APIs

Authorised third-party developers and service providers can use the marketplace APIs to enable new services on the Reltime platform. For example, a third-party developer can build and deploy an eKYC verification or credit scoring tool using the marketplace APIs. See the list of APIs in the appendix.

6.3 Partner API access

Partners of Reltime can access the partner APIs. The secured partner APIs can enable partners to embed certain Reltime services within their existing services and offerings. For example, fintech partners can enable Reltime lending functionality in their app offering.

6.4 Partner full tenant

Reltime can provide complete hosting services for selected partners to use its full services and infrastructure. For example, financial institutions in emerging markets can use Reltime's entire services and infrastructure.

6.5 Technology layers

Reltime's operations are executed through a technology layer that includes Open Banking / PSD2 integration, a high-speed blockchain infrastructure, an efficient back-office platform and an advanced data engine.

7 How it works

Reltime's ecosystem operates with the digital currency[14] as the base instrument for payments and other transactions. Reltime has built loyalty functionality that can be used for attack functionality based on a listed token called RTC.

[14] https://news.cision.com/reltime-as/r/reltime-enables-merchants-to-accept-payments-in-digital-currencies-and-cbdcs-globally,c3986612

7.1 Design approach: MTDPoS Protocol

Reltime has the functionality described here up and running. Point-of-sale, or POS transactions, are the key elements leading to digital transactions. The following article will give brief information regarding the moving target POS.

With the development of technologies and advancements, money transactions are not only physical exchanges on a scale. You can make secured transactions with just a click and swipe away. This seems like a game, but this is what reality is in the digital world. With economies going cashless, the POS systems help meet the demand for swipes and plastic money. The POS functions as the digital transaction gateways, which are also effective in providing secure transactions. For all digital transactions, security is critical so that money is not used in the wrong way of commerce—preventing unauthorised access to electronic gateways by individuals looking to steal personal information from the users. Creating a secure environment for customers to complete their transactions is vital to protect information from unauthorised access.

Cryptocurrency has made it extremely easy to transfer funds, buy commodities, and make transactions between two parties using ledger accounts in the form of digital tokens. They allow safe and encrypted online transactions, saving time and energy. There are more than 6,700 different cryptocurrencies, including Stellar (XLM), Ethereum (ETH), Litecoin (LTC), Bitcoin and many more. Based on a report submitted by CoinMarketCap, the total of all cryptocurrencies is around USD 1.6 trillion. One of the most feasible and acceptable measures for cryptocurrency use is the nonparticipation of banks. Initially, to buy cryptocurrency, one has to credit real money in exchange for virtual money. After that, transactions can be made with other cryptocurrencies.

7.2 The MTDPoS Design

The information is kept secure and encrypted; information is made public because of blockchain. Blockchains contain a list of people involved in public transactions. While looking at the return policy, the use of virtual currency has been debatable. Since the value of digital currency keeps changing, as the price of stocks, refunds offered with cryptocurrency as a medium of exchange may lead to losses. All countries accept cryptocurrency as a legal digital transaction measure. The legal rules, laws, and rights regarding the purchase and sale of this exchange form are not the same everywhere, leading to the discrepancy.

As a technical, virtual, and digital medium of exchange, cryptocurrency has become a new and exclusive means of transaction. It works on blockchain Networks to provide flexibility regarding usage and conduct. It finds miners, blocks, nodes, nonce, and hash to provide a high level of security, ensuring Transactions in the form of coins and commodities. A proof of stake consensus algorithm makes mining subtle and straightforward by reducing the chances of theft. Proof of Stake doesn't require miners to produce new coins even if a transaction occurs. Instead, it works with participating nodes such as validators. It is also environmentally friendly as the issue of high energy consumption is finding a way out.

Leads. Hacking can be similar to a computer hack. Hackers have started installing malware in the devices of the POS terminals, which has given cybercriminals access to steal consumer payment information, leading to huge losses. The hackers install a moving device for monitoring the POS system to steal payment information. The retailers and POS system owners face defamation and heavy lawsuits.

8 Technical field

The present disclosure relates to blockchain networks' systems, methods, and techniques to improve systems, processes, and strategies for handling scalability, protocol diversity, and identity verification.

8.1 Proposed protocol for use in Reltime

Reltime has chosen to integrate several protocol possibilities.

- For the B2C approach, RTC (listed token)
- Reltime also support minting digital currency and CBDC
- For the B2C approach, the digital currency(a stable token based on Proof of Deposit and mechanism for backing by the central bank)
- For the protocol used for transport within the ecosystem, a customised Reltime PoA blockchain is named MTDPoS. The supported protocol supports less than 2 seconds on average, while Mastercard supports less than 2 seconds on average, meeting Mastercard's demand for contactless payments.
- As Reltime is a Layer 1 blockchain. For B2B2C, whitelabel and OpenAPI, Reltime's partners can develop their token(s).
- For dApps, Reltime, this is the marketplace service.

8.2 Proposed Protocol, ecosystem

The new protocol describes a new architecture where the Multi-Tenancy is a part of the Delegated Proof of Authority.

The goal of the organisation, using the Multi-Tenant Delegated Proof of Authority, is to deliver blockchain transactions with 300ms -2sec [15]. Based on location, this speed can stop a contactless transaction if you are outside a trusted zone. It prevents all transactions, money flow, and accounts from being hacked. It handles transactions, accounts, and money flow to the third party. In Multi-Tenant Delegated Proof of Authority, the node at which the consensus will be voted democratic by all the tenant users. Before storing the data in either a public or global blockchain, the data is encrypted using a Multi-Tenant Delegated Proof of Authority. Each tenant has their permission blockchain, and each blockchain has its trigger for writing data to the corresponding blockchain, so the transaction on one chain would not affect others.

The other role can also eliminate the functions of witnesses, which are different roles. Blocks. Witnesses create and validate blocks in some Delegated Proof of Authority-based blockchains. The most popular witnesses become part of a block forger committee. For every validated transaction, the witnesses in the top tier are awarded fees. Most of the Delegated

[15] https://news.cision.com/reltime-as/r/transactions-in-under-2-seconds--that-s-how-quick-reltime-baas-is-,c3496476

Proof of Authority based cryptocurrencies do not allow the witness to prevent transactions from happening. The witness is redirected to the next active witness immediately when a witness misses a block. The witness might miss the block when the server goes offline.

In Multi-Tenant Delegated Proof of Authority, the tenants must agree to use the same blockchain platforms, consensus algorithm, and configuration, or they have the flexibility to choose different blockchain platforms. The tenants can register a unique ID, metadata, and scan events. They can read all the historical events and data values over time. The different tenants can have different needs. In such cases, Multi-Tenant Delegated Proof of Authority offers multiple tenant platforms. Multi-Tenant Delegated Proof of Authority can achieve data integrity, low cost, performance, and isolation.

In Delegated Proof of Authority, some witnesses are offered a right to block transactions by some cryptocurrencies. Even after giving the witnesses the rights, the malicious use of the power is prevented. It is prevented by active voting and possible reputational damage. The witnesses in Delegated Proof of Authority blockchain cannot change any information about or within a transaction. The purpose of voting delegates is to govern the system and propose core changes. They oversee parameters such as transaction fees, witness pay, block sizes, and block intervals of the network. They are the parameters that are under their competence and not paid positions. They can propose changing the size of the block or the amount a witness should be paid. The blockchain then votes on their proposal to adopt the change. The proposed changes come into effect only when the users approve the changes.

The anchoring scheduler was arranged between the tenants and the platform owner as agreed. With the help of the genesis block, the individual and unique identity of each blockchain is well established. The initial step of the protocol involves querying and verifying the newest Merkle root saved on the public blockchain against the tree in the anchoring component. This step helps us know if the element is up to date—all the subprocesses for the tenant's authorised blockchain run in parallel order. Querying of the Blockchain Merkle is carried out at the latest block. A tenant chain's root is not updated if the node timeout is unavailable. Once all the blockchains are processed, the protocol wires the Merkle Root of the latest tree of roots to the public blockchain.

During the design phase, tenants with greater transactional capacity and throughput are more likely to affect the performance of less efficient tenants since all the data is stored in one blockchain trigger. On the other hand, transactions based on one chain would not affect others as tenants have personal permission blockchains, each consisting of a unique trigger for printing data on the blockchain. Those designs using a public blockchain will be able to achieve availability. Availability can be increased by adding more full nodes and block generators. An increase in tenants also increases the cost of infrastructure and its maintenance overhead. Isolation is one of the essential functions; tenants should only be allowed to read their data and not competitors. To ensure the segregation of data, information is disguised using encryption. Blockchains are used as a neutral data store to keep a piece of unique ID information. Anyone can use deployed intelligent contracts on the internet to access the information stored inside this unique information ID. Local blockchain nodes and the blockchain triggers are hosted on one virtual machine.

This protocol system is faster than traditional proof of stake and proof of work systems. Unlike the proof of work system, it does not require much electricity for proper functioning. Since no extra or specialised equipment is used in the process, it is cheaper and more accessible to become a user, witness or delegate.

Delegated Proof of Authority system structure and incentives strengthen the integrity and security of the entire blockchain network, and each gets incentives to do their job honestly. A proof of work mechanism works by having all nodes solve a cryptographic puzzle. Miners solve the unknown, and the first one to decrypt the code gets rewarded. This has led to a situation where people build larger mining farms. These mining farms are a great consumer of electricity. According to research, these farms use the power equivalent to five million households in the US or the power consumed by New Zealand. This mechanism gives more rewards to people who have better equipment. The higher your hash rate is, the higher the chance you will create the next block and receive the mining award. People started using the mining pool technique, where miners combine their hashing power and distribute the reward evenly across everyone in the pool. Mining is the process of adding the records of recent transactions to the blockchain ledger after thoroughly checking and analyzing the validity of the transactions. The transactions are verified with the help of complex hardware, which further carries out complex mathematical calculations. The computer miners are assigned to check the validity of the transactions, and only if the transaction is found to be genuine, is it added to a secure block. These blocks are then used to form a blockchain. Once a hash is created and assigned to each block, the miners that made it possible are rewarded with bitcoins.

To solve the above issues, a forum user of Quantum Mechanics proposed a technique called proof of stake. The core of this idea is that letting everyone compete against each other in mining is wasteful. Mining is essential because it avoids double-spending bitcoins. Hence, this consensus mechanism chooses one node out of all to validate the next block. Instead of allowing blocks to be mined, the protocol allows the forging of a partnership. The application of fixed length and mathematical algorithms helps in the generation of new value.

- Hashing creates a different identity that is used for sensitive information. It has parallels to the protection of the password. With a unique hash on each node, the private key having access to the sensitive information is converted into a public key through hashing. It helps users send data or information to their destinations without fearing theft. Mathematically, hashing is nearly impossible to decode. Validators are not chosen randomly. To become a validator, a node must deposit a certain amount of crypto coins into the network to prove commitment. It can also be considered as a security deposit. Validators will lose a part of their stake if they approve a fraudulent transaction. If the stake is higher than the transaction fees, we can trust them to do their jobs honestly. It is unlikely that someone would lose a more significant amount of money to get a smaller amount. This is a financial motivator for the validators. Once a validator is removed from their position, the transaction money and stakes are released after some time. This extra time is to check out all the transactions before you get your money and leave.

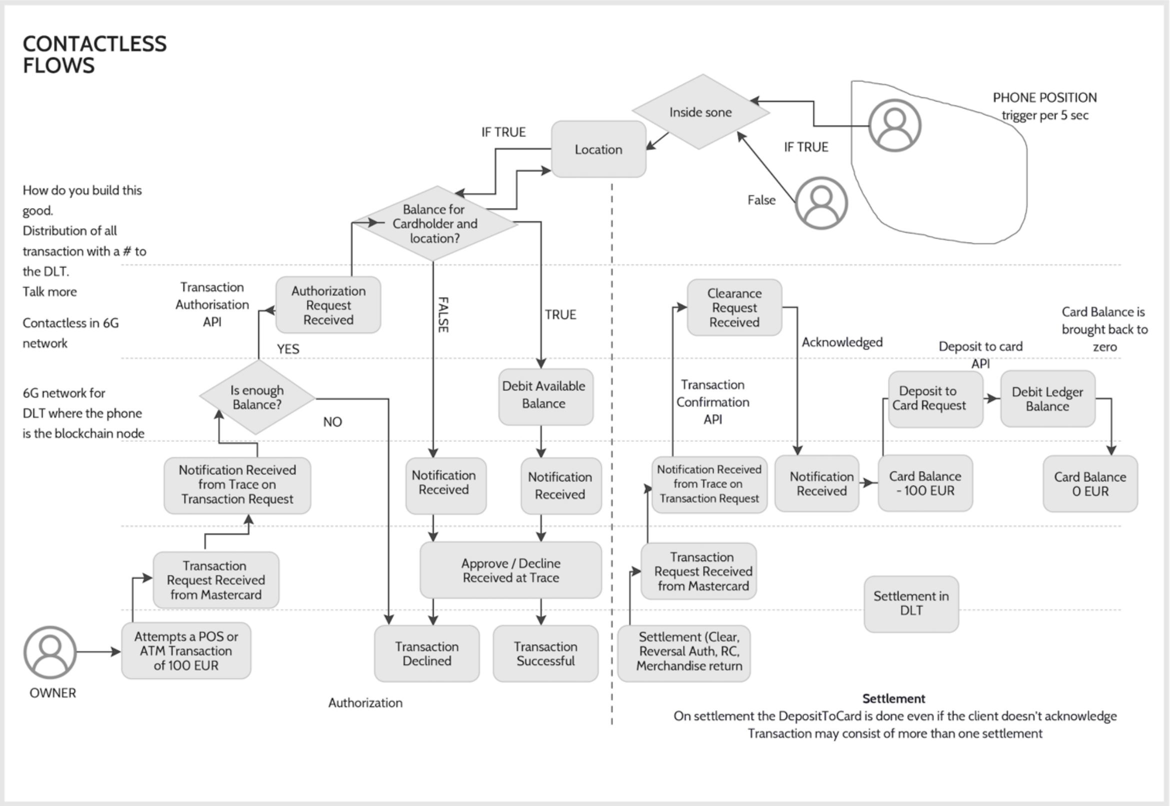

CONTACTLESS FLOWS
How do you build this good.
Distribution of all transaction with a # to the DLT.
Talk more
Contactless in 6G network
6G network for DLT where the phone is the blockchain node
OWNER
Attempts a POS or ATM Transaction of 100 EUR
Transaction Request Received from Mastercard
Notification Received from Trace on Transaction Request
Is enough Balance?
YES
NO
Transaction Authorisation API
Authorization Request Received
Balance for Cardholder and location?
IF TRUE
Location
Inside sone
IF TRUE
False
PHONE POSITION trigger per 5 sec
FALSE
TRUE
Debit Available Balance
Notification Received
Notification Received
Approve / Decline Received at Trace
Transaction Declined
Transaction Successful
Authorization
Clearance Request Received
Acknowledged
Transaction Confirmation API
Notification Received from Trace on Transaction Request
Notification Received
Transaction Request Received from Mastercard
Settlement (Clear, Reversal Auth, RC, Merchandise return
Deposit to card API
Deposit to Card Request
Debit Ledger Balance
Card Balance is brought back to zero
Card Balance - 100 EUR
Card Balance 0 EUR
Settlement in DLT
Settlement
On settlement the DepositToCard is done even if the client doesn't acknowledge
Transaction may consist of more than one settlement

Figure 6: Contactless flows

The name derives from the fact that a microtransaction purchase is small in amount and function. In micro transactions, the price is often no more than USD 10. It may range from less than 99 cents to USD 10, but it is mainly supplemented by selling in bulk.

The contactless payment systems are multi-tenant delegated. The smart cards can be used for multiple purposes, such as identifying and storing data and information, authentication, providing practical business transactions, and reduced human interventions. The contactless payment intelligent cards do not possess a battery but have a built-in inductor where the incident electromagnetic signal is captured. The electronics of the smart card are powered through it. The multi-tenancy of the contact payment systems is seen through the producers of smart wristbands, smart cards, fitness trackers, key fobs, and smartwatches, besides the common smartphones. For the security of the customers' data and information, a different numeric value is used in place of the customers' primary account number, which is called a token. It is an effective tool to reduce data breaches and fraud.

Contactless payment is the primary medium, payment method for tickets in many cities such as Seoul, the UK, Tokyo, and Hong Kong. Retailers. Retailers are putting forth processes and infrastructures to implement the contactless payment systems. The ongoing costs are considered, including costs for upgrading POS software and hardware systems, training of the service staff for customers, transaction, marketing, promotion, and expenses relating to the management and maintenance. The multi-tenancy and protocol of the contactless payment help support any virtual processes relating to the payment and purchases, including all the costs of the traditional credit and debit stored value payment and account-based payment, which is pre-authorised. The participation of one or more finance institutions is needed for credit and debit transactions. Contactless payment methods have become more prevalent, with frequent usage in public transportation, restaurants, bars, cafes, and online and offline purchases. There are two types of pre-authorised accounts. For one account, transactions are directly processed by the institution, while for the other, pre-defined transactions are brought about, which is replenished when the lower value limit is reached. Hence, the protocols include:

- A strong understanding of the maximum value of the transaction.
- The liability of frauds.
- The application of the transaction fees.
- There are various types of online processing and networking.
- The availability of technologies proven for the implementation.

Examples of companies using the contactless payment systems for operating the transportation for passengers and in the business places through the payment through smartphones and other intelligent devices, supported by NFC, show the importance and convenience of the contactless payment systems for companies and ordinary users in everyday life. The right technology should be selected and implemented to support its commercial availability, whether it possesses the potential and ability to support its commercial availability, and whether the technology possesses the potential and ability to help similar similar payment applications. Understanding the total ownership cost for any system is crucial.

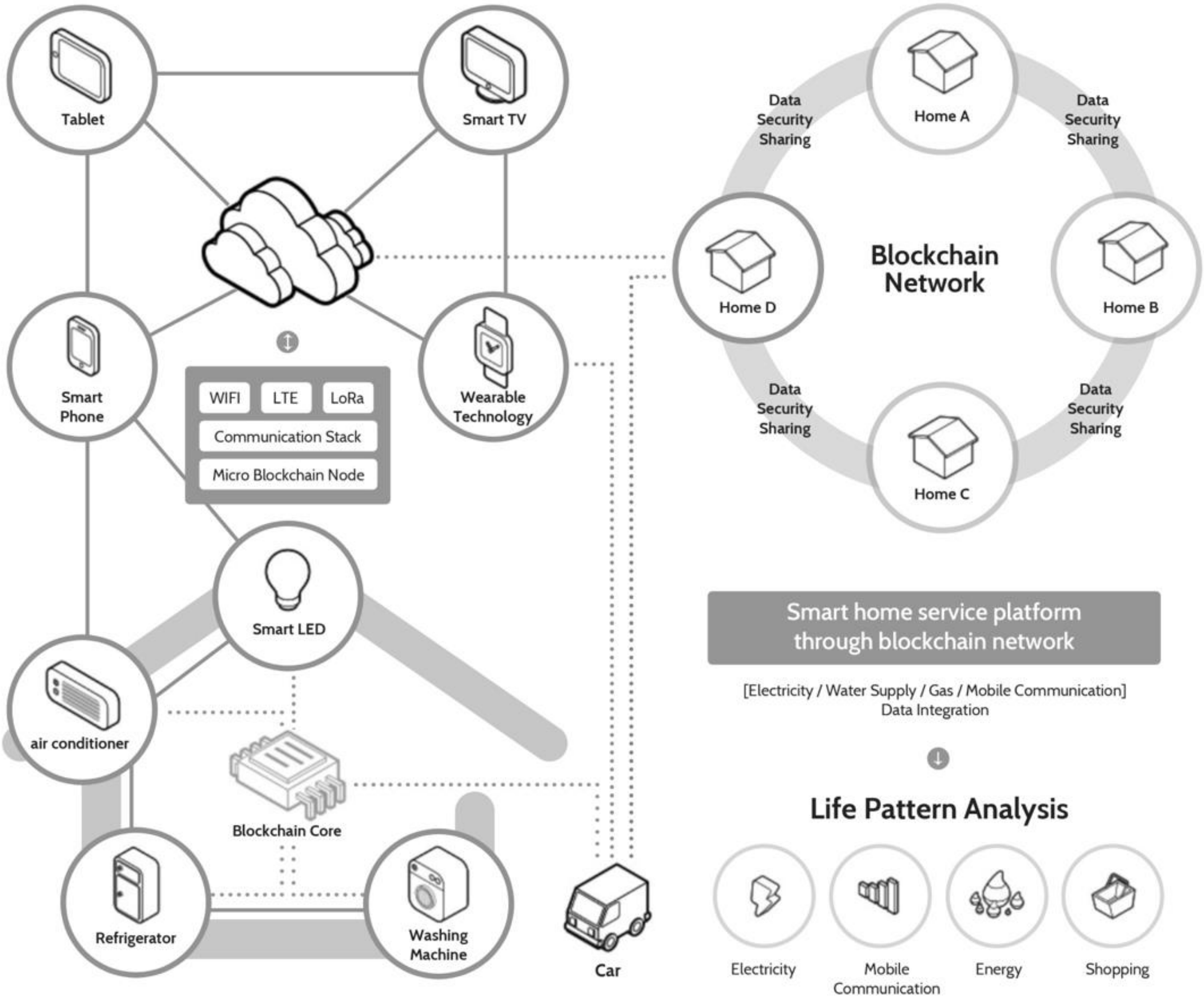


Figure 7: Where the micro transaction is ahead

Micro transactions are often called the most player-unfriendly application of business practice.

Every blockchain needs a consensus mechanism to ensure the truth and honesty of records. The three most commonly used consensus mechanisms are proof of stake, proof of work, and authority. In explaining the staking mechanism, the creator of a new block, also known as a validator, is randomly chosen based on how much stake they commit to the network. Thus, the higher a stake placed, the higher the chance to be selected as a validator. Designing a multi-tenant blockchain system is comparatively tricky for architects of performance, isolation, and scalability. In a multi-tenant scenario, providing isolation of transactions is quite essential. One tenant should be able to read or write into another's data. This system requires scalability on an individual and non-individual level while maintaining data integrity, performance, and isolation.

Since. NFC is the chief player, mobile handset manufacturers gain a commission and other significant economic benefits from implementing mobile-based payment applications. MHMs are offered hefty money from financial industries to provide cashless payments and add default payment apps. Furthermore, seeing the security and other benefits of cashless transactions, more and more people turn to buy devices with such chips, increasing the company's sales.

8.3 Reltime—Introduction new State of the Art for digital transactions

In this segment, there is a demand from the financial sector to support a maximum speed for a single transaction[16] The main focus for digital currency is transaction volume per second. In principle, on average, today's Public DLT solution supports Mastercard or Visa transaction time of <2 seconds.[17]

Payment providers have defined a comprehensive set of approval processes based on the MCBP specifications to support the deployment of solutions such as Mastercard.[18]

Developers developing their MPA.[19] According to MCBP specifications, functional testing must be completed before provisioning any live devices successfully.

While the transaction performance test will be informative, issuers should be aware that for M/Chip transactions, cards and mobile phones must meet targets of <2 seconds in average. Transaction performance is a critical parameter in the user experience for all types of payments, especially in public transport use cases.

8.4 Smart contracts

- It helps with predictions and supports the prediction markets. The users can make P2P intelligent contracts that can be unlocked if any particular event applies to the insurance industry. The traditional money allows individuals to decide the conditions in which payments can be made.

- It examines the benefits of distributed ledger technology (DLT). It also aims to centralise the database and transfer of networks for an interconnected economy.

8.5 Detailed description

Figure 8 represents a block diagram instance of an embodiment of a transaction tracking system. It is in a peer-to-peer network situation. A representation of a non-limiting embodiment of a system tracking system involves at least one transaction block generator suite. Besides, it is also equipped with one trusted digital identity issuer system. They are in touch with various other peer-to-peer nodes in the framework situation. There is an inclusion of several blockchain peer-to-peer nodes which are not depicted in the network environment. They perform

[16] https://news.cision.com/reltime-as/r/reltime-defi-ecosystem-is-shaking-things-up-with-a-switch-to-poa-based-blockchain-network--a-first-i,c3489637

[17] AN 1426—Introduction of Transaction Performance Testing to MPA Issuer, Self-Test Process, Generated on 20 May 2019 Published on 29 January 2018

[18] Mastercard AN 1426—Introduction of Transaction Performance Testing to MPA Issuer Self-Test Process Generated on 20 May 2019 Published on 29 January 2018

[19] 19 AN 1426—Introduction of Transaction Performance Testing to MPA Issuer, Self-Test Process, Generated on 20 May 2019 Published on 29 January 2018

different functions as well as subsets of operations. In addition, there are also a few electronic transaction devices a-m. Besides, the various nodes of a peer-to-peer network environment are paired communicatively through a distributed communication network.

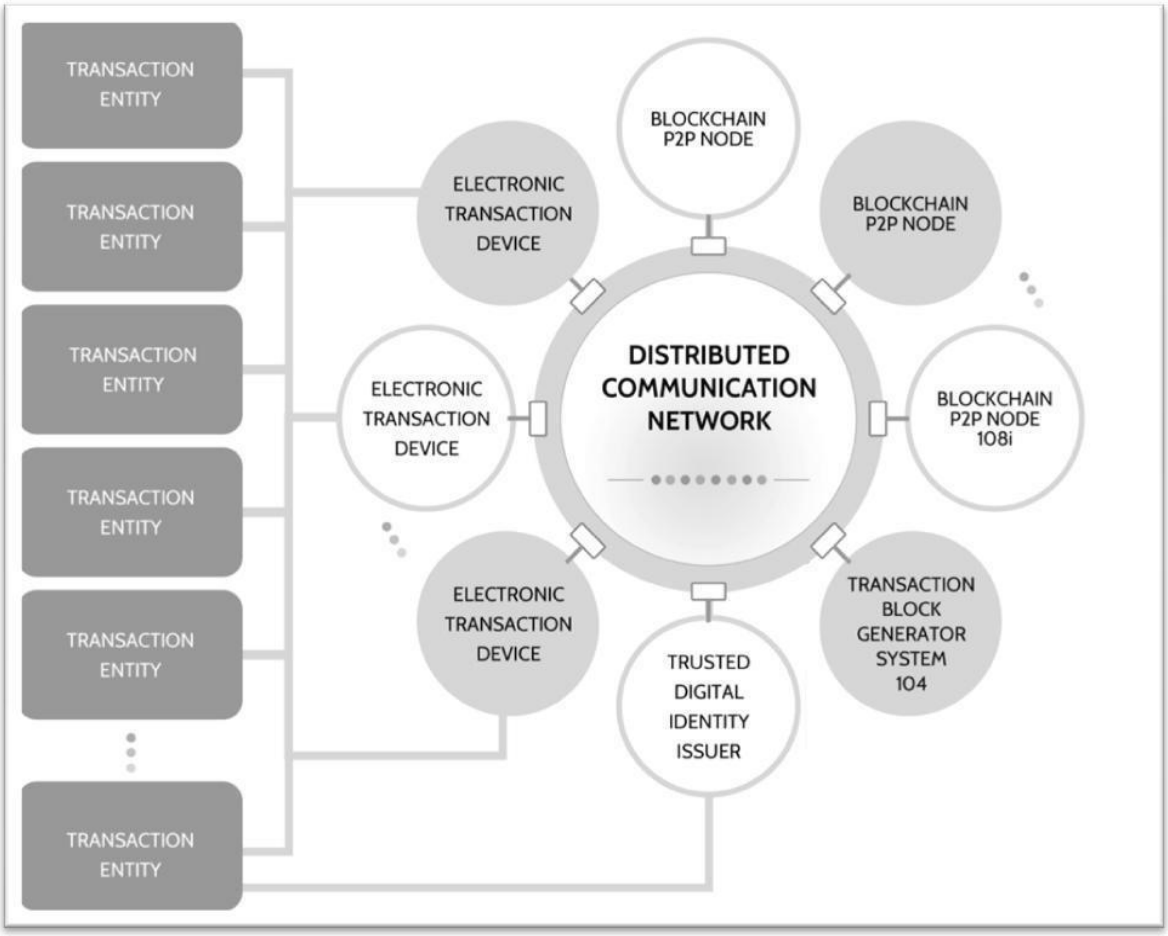

TRANSACTION ENTITY
TRANSACTION ENTITY
TRANSACTION ENTITY
TRANSACTION ENTITY
TRANSACTION ENTITY
TRANSACTION ENTITY
ELECTRONIC TRANSACTION DEVICE
BLOCKCHAIN P2P NODE
BLOCKCHAIN P2P NODE
ELECTRONIC TRANSACTION DEVICE
DISTRIBUTED COMMUNICATION NETWORK
BLOCKCHAIN P2P NODE 108i
ELECTRONIC TRANSACTION DEVICE
TRUSTED DIGITAL IDENTITY ISSUER
TRANSACTION BLOCK GENERATOR SYSTEM 104

Figure 8: Block diagram instance of an embodiment of a transaction tracking system

Is responsible for creating a block of a blockchain. A blockchain is commonly an immutable transaction ledger. It is well-maintained inside a distributed peer-to-peer node network. Each of these peer-to-peer nodes is responsible for maintaining a copy of the catalogue. They do so by executing a transaction that the consensus pool has authenticated. The catalogue is then divided into various blocks, each containing a hash that combines every block with the block in front of it. All these linked blocks are then known as the blockchain.

A generic communication system is depicted through the distributed communication network. This network contains a cellular telephone system like a radio frequency wireless system in an individual embodiment. Likewise, a suitable transceiver is included in several environments. This peer-to-peer network environment can also be a telephony system, internet LAN system, or even a WIFI system, among other alternatives. It can also be a cellular system, an infrared system, or even a hybrid system consisting of several different communication media. One can also implement the Member devices of this peer-to-peer network environment for communication. These communication purposes can be served by using various communication technologies. These technologies are digital subscriber loop (DSL), X.25, Internet Protocol (IP), Ethernet, Integrated Services Digital Network (ISDN), and asynchronous transfer mode (ATM). However, they are not limited to these technologies. All the embodiments presented for the distributed communication network can be configured communication to communicate over combination systems. They have several segments that can employ diverse formats technologies for every segment.

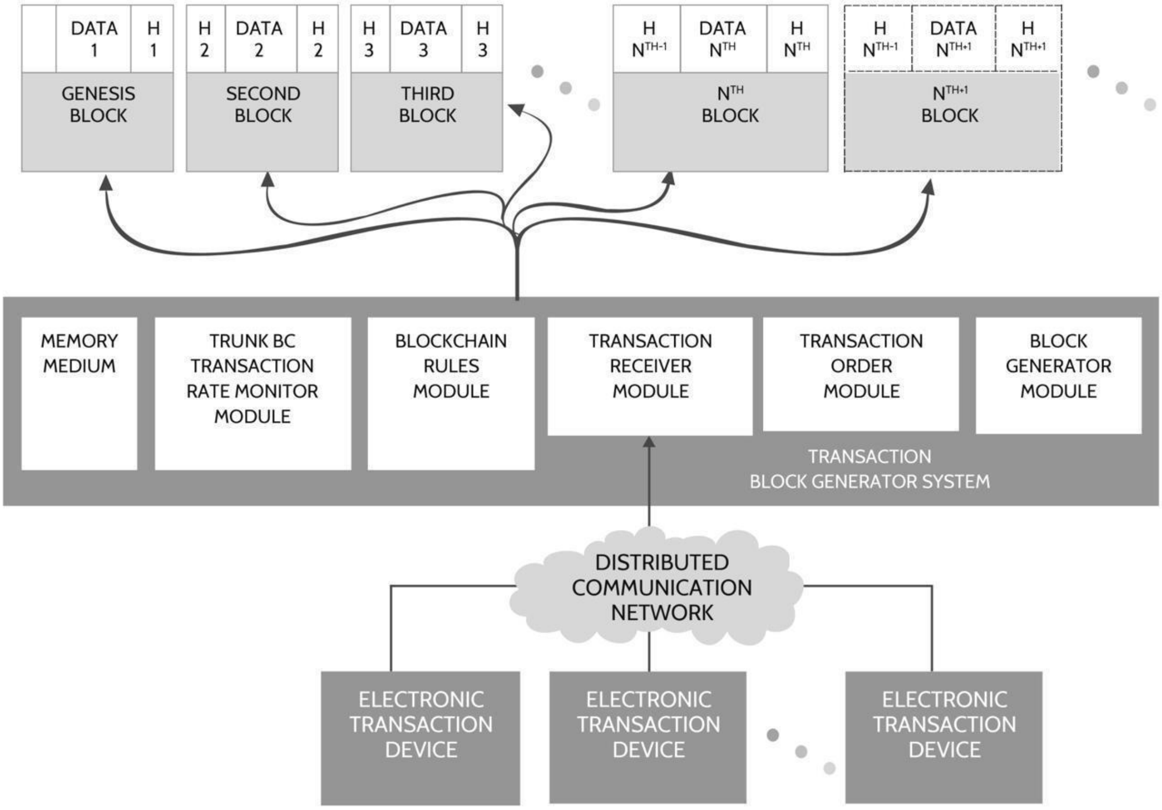


Figure 9: Block diagram that displays details of the transaction block generator system

Figure 9 is about the block diagram that displays details of the transaction block generator system. It involves a transactor receiver module 2021, a transaction order module, a block generator module, a trunk blockchain (BC) transaction rate monitor module, a blockchain rules module, and a memory medium. On the other hand, other embodiments consist of unseen blocks and modules (not shown) that are responsible for different functions. Moreover, some blocks of the figure can also be integrated with other blocks or modules. One can also implement blocks or modules of figure 9 as hardware, firmware, or a combination of hardware and firmware in multiple other embodiments. In contrast, the blocks or modules of a transaction block generator system104 can be implemented in a distribution in a few embodiments. This process can be done using several peer-to-peer gadgets interconnected through the distributed communication network.

Besides, the transaction receiver module communicates with the distributed communication network, the transaction block generator system, and the plurality of electronic transaction devices. The transaction details for the finished transaction are transmitted to the transaction block generator system when the marketing is done by one of the electronic transaction devices. The transaction receiver module recognises each received transaction information. The transaction receiver module adds supplemental data of interest interlinked with the data received about the transaction in a few embodiments. An identifier that identifies the information in the transmission of electronic transaction devices to the transaction information, which can be sorted as an example. The timestamp is also supplemental data. For instance, a geographic location recognises the time and place of transacting and the area where the transaction information was generated or received. Every kind of data that is well-suited can be embedded into transaction information. It can be done, that is, into the information, or as associated metadata, that is, into the information, or as associated metadata.

There are also a few embodiments wherein several transaction receiver modules help pair several electronic transaction devices. One good example would be using diverse communication formats and providing the transaction information in various forms by several electronic transaction devices.

- Figure 10 describes a block diagram that shows extra detail of the transaction block generator system. It shows the designed branch transaction block generator system. Branch transaction block generator system consists of various things such as a branch transaction receiver module, a branch transaction order (T-Order), a branch block generator module, a branch blockchain (BC) transaction rate monitor module, a branch blockchain rules module, and a branch memory medium to name a few. These components share features that are similar to those of the branch transaction block generator system. Both of these also share similar reference numerals that tend to recognise these components. These modules or blocks of branch transaction block generator systems are not defined in detail as their operation and functions are typically or at least significantly similar. Likewise, other unseen embodiments consist of blocks or modules that offer different functions. Besides, some blocks and modules presented in blocks. Figure 11 can be combined with other blocks, others, or both. The modules displayed in Figure 11 may be implemented as hardware, firmware, or a combination of hardware and firmware in the various embodiments. Whereas in a few embodiments, branch transaction block generator system blocks can be implemented in distribution. It can be done using several peer-to-peer devices networked through the distributed communication network.

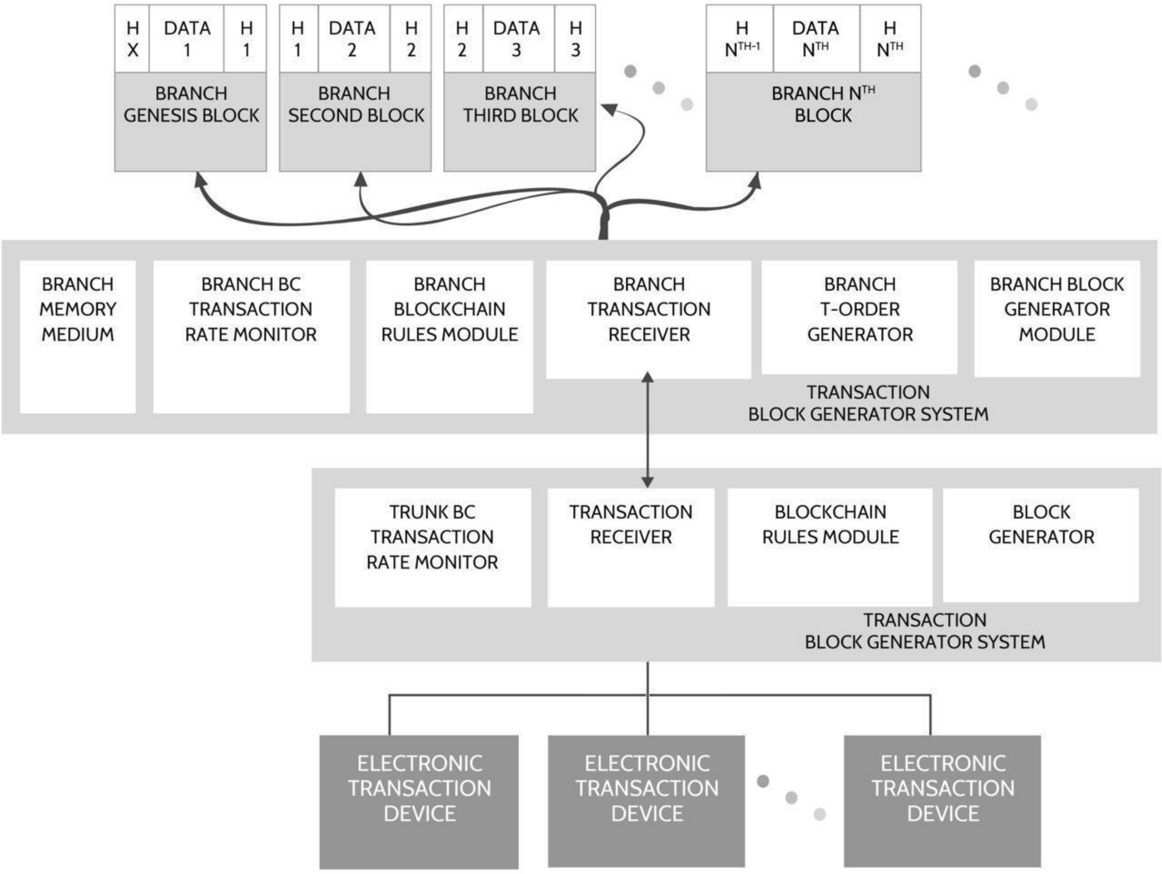

H X
DATA 1
H 1
BRANCH GENESIS BLOCK
H 1
DATA 2
H 2
BRANCH SECOND BLOCK
H 2
DATA 3
H 3
BRANCH THIRD BLOCK
H N^TH-1
DATA N^TH
H N^TH
BRANCH N^TH BLOCK
BRANCH MEMORY MEDIUM
BRANCH BC TRANSACTION RATE MONITOR
BRANCH BLOCKCHAIN RULES MODULE
BRANCH TRANSACTION RECEIVER
BRANCH T-ORDER GENERATOR
BRANCH BLOCK GENERATOR MODULE
TRANSACTION BLOCK GENERATOR SYSTEM
TRUNK BC TRANSACTION RATE MONITOR
TRANSACTION RECEIVER
BLOCKCHAIN RULES MODULE
BLOCK GENERATOR
TRANSACTION BLOCK GENERATOR SYSTEM
ELECTRONIC TRANSACTION DEVICE
ELECTRONIC TRANSACTION DEVICE
ELECTRONIC TRANSACTION DEVICE

Figure 10: Block diagram that shows extra detail of transaction block generator system

In some representations, system (branch transaction block generator) and system (transaction block generator) are executed on separate information processing systems. However, in many other representations, the system, the branch transaction block generator, and the system, which is a transaction block generator, are executed on the same information processing systems.

It is possible to make several branch transaction receiver modules. They can be created either based on needs and based on desire. Moreover, it is possible for the representations of a system, the transaction tracking system, to have an appropriate number of systems (branch transaction block generator). Often, transaction rate saturation issues occur, which can be reduced by generating a new branch transaction block generator system. On the other hand, new branch transaction block generator systems of any type, based on any rule like protocols, techniques, processing of transactions, can be introduced.

As soon as the branch blockchain is generated, the branch transaction block generator system close. It means that the device responsible for running the branch transaction block generator systems can stop the production of new blocks for the branch blockchain. Instead, it can start other procedures and functions which are in no way related to the system.

After seeing figure 11, people might wonder what it is. It is, in fact, a contextual demonstration of trunk blockchain that is responsible for generating various branch blockchains at different intervals of time. No matter which blockchain it is, the first block of the trunk blockchain is the genesis of that blockchain itself. Typically, the first block is the trunk blockchain. So, it is the genesis block.

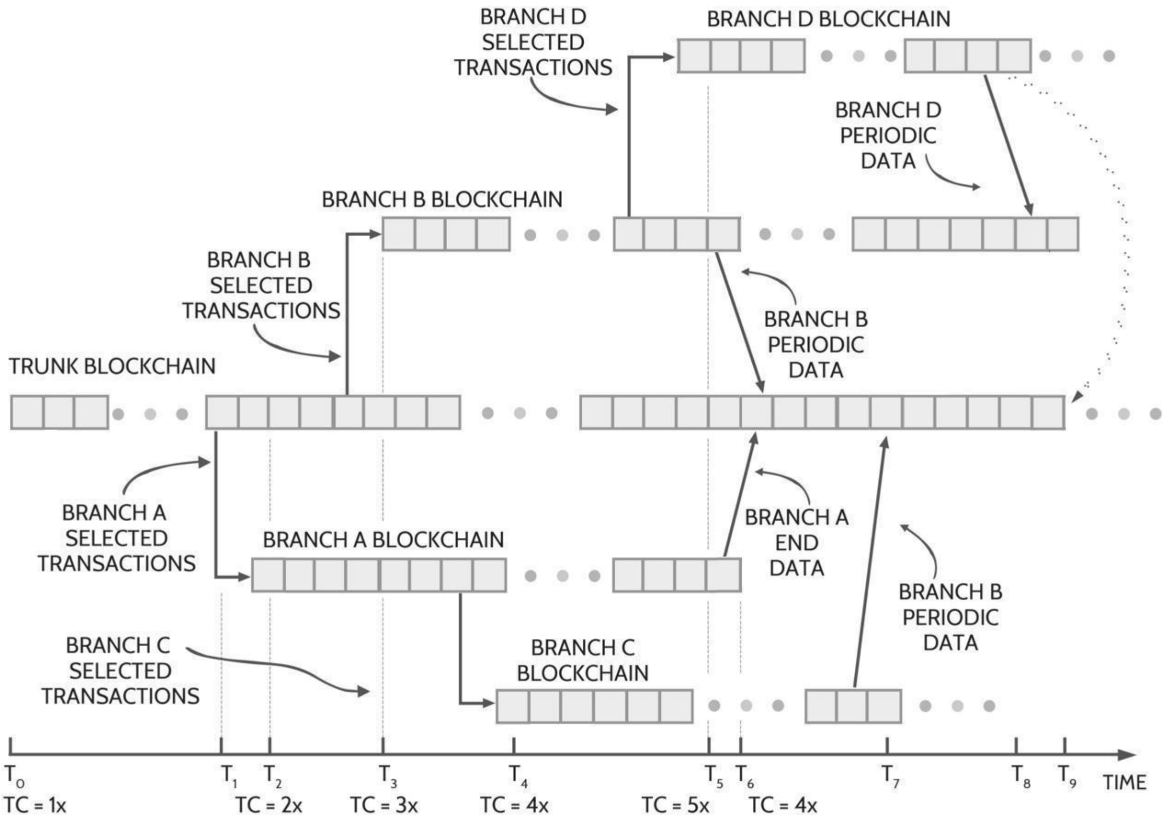


Figure 11: MTDPoS

At any point in time T1, an occasion will come that will leave no choice but to initiate the emergence of the first branch blockchain. After it is named "Branch A Blockchain." It has been shown in figure 12. The process of generating a series of branch blockchains is portrayed and explained to resolve saturation in legacy blockchain systems. Nevertheless, anyone skilled in the art will appreciate that with the representation of the transaction tracking system, any branch blockchain can be generated for any event or rule.

Just for the sake of discussion, assume that any time before the conceptual time decided above (T1), the trunk transaction tracking system, which is responsible for producing the trunk blockchain, outreaches or approaches the saturation level of the transaction rate. If this occurs, the trunk transaction block generator system will start generating a new branch transaction block generator system. It has been depicted in figure 11. The process takes place so that the system, which is newly created, becomes capable of generating new blockchains at any time, let's say T2. It can be denoted as Branch A Blockchain. Then, the system, which is the trunk transaction block generator system, chooses a particular segment of entering transaction information. This transaction information can be called 'branch A selected transactions. This is then handled by the system, which is the new branch transaction block generator. After the completion of this process, it is stored in the Branch A Blockchain. After a block is generated in the trunk blockchain, the computation of the ending hash value of the block takes place. After this, that particular hash value along with any suitable information which the person wants to store in the block (initial genesis block) is sent to the new branch transaction block generator system. The further process depends on the representation. Based on that, the new branch transaction block generator state gets hold of the transaction information. This happens in such a way that a new genesis block is formed. This new block saves all the transaction information that was acquired by the new branch transaction block generator. The hash value of the block is also saved in the genesis block. The process is shown in figure 12.

The saturation problem is paid heed to. With reference to this, after the Branch A Blockchain has been formed, the TC, that is the transaction rate capacity is increased. In this case, the maximum total TC (transaction rate capacity) will be twice as much as the TC of the authentic trunk branch. This is because a new branch transaction block generator system is available to save and look after the rest of the incoming transaction information. It is assumed that the technology used by both block generator systems is the same or almost the same. However, the new incoming transaction rate capacity might increase or decrease depending upon the incoming information regarding the transaction. This transaction information is sent to the new branch transaction block generator system. system generates and manages the Branch A Blockchain.

Carrying on with the example shown in figure 12, assume that there is a time before T3. The trunk transaction block generator system, which is responsible for forming the trunk transaction, becomes saturated again. To lower the transaction rate saturation, one needs a new transaction block generator system is introduced. After a certain period, let's illustrate it as T3, it is noticed that the new transaction block generator system forms the first new genesis block.

The whole process and effects described above are for the first branch, A blockchain. These processes and products are equally applicable to the second branch, B blockchain generated recently, and the new transaction block generator system. In this case, the maximum total transaction rate capacity is three times the original TC of the plan (trunk transaction block generator). The system is responsible for making the trunk blockchain.

Looking at the example that has been illustrated in Figure 12, one will notice that there are a total of five operational blockchains. These blockchains are responsible for processing, storing, and managing the incoming transaction information. When the maximum total transaction rate capacity is calculated now, it is five times the original TC of the system (trunk transaction block generator), which is responsible for making the trunk blockchain.

Some of the tracking system's representations help provide novel features. As said earlier, the system is responsible for making the trunk blockchain. It is a process of periodically gathering information, where either some or all the data stored in the branch blockchain is collected. It is then returned to the system (trunk transaction block generator). After this process is finished, the total information generated can be sent for storage to the trunk blockchain's new branch (which will be generated).

Yet another novel feature of the tracking system is that there is a possibility that the process of generating and managing the blockchain might end at any suitable time. For instance, it is possible that at time T, it is decided that the formation of blockchain A is no longer a need. Block would be the last generated block, and it would be the end of the blockchain. In that case, the formation and management process can be stopped then and there.

Someone skilled in the art would acknowledge that when a blockchain is ended, it will result in an available curtailment of the maximum TC if there is a need to conserve either memory or computing resources.

Alternatively, the system might allow one of the blockchains to be deleted. It can be a branch of blockchain. All the information that was stored in branch A can be sent to the main trunk for storage.

In some incarnations, a gather-up process is likely to be performed on a child branch blockchain. The gathered-up information is expected to be communicated to the trunk transaction block generator system for incorporation into a block of the truck blockchain. For instance, at a time T7, a gathering process is performed by the branch transaction block generator system managing the Branch C Blockchain. The information may then be incorporated into blocks, for e.g., generated by the trunk transaction block generator system.

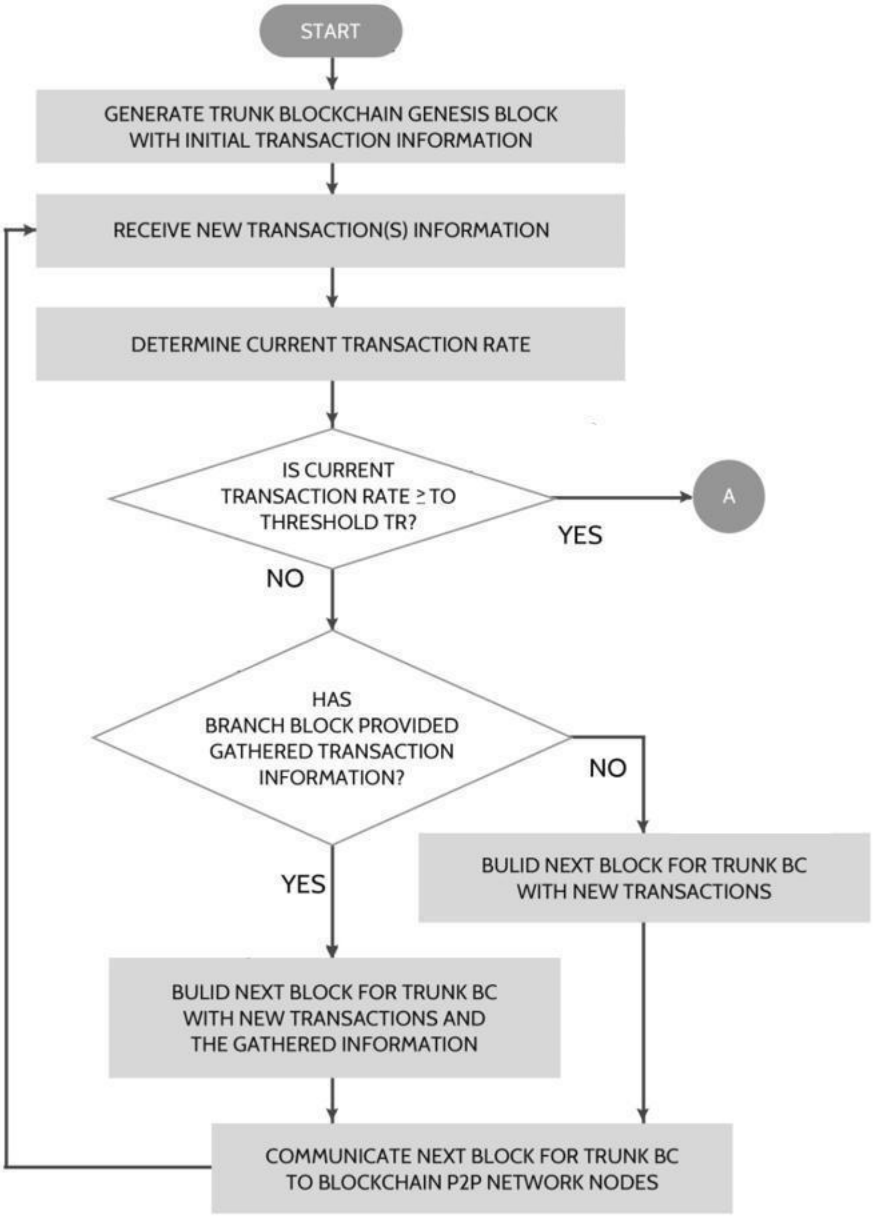

START
GENERATE TRUNK BLOCKCHAIN GENESIS BLOCK WITH INITIAL TRANSACTION INFORMATION
RECEIVE NEW TRANSACTION(S) INFORMATION
DETERMINE CURRENT TRANSACTION RATE
IS CURRENT TRANSACTION RATE ≥ TO THRESHOLD TR?
YES
A
NO
HAS BRANCH BLOCK PROVIDED GATHERED TRANSACTION INFORMATION?
NO
BULID NEXT BLOCK FOR TRUNK BC WITH NEW TRANSACTIONS
YES
BULID NEXT BLOCK FOR TRUNK BC WITH NEW TRANSACTIONS AND THE GATHERED INFORMATION
COMMUNICATE NEXT BLOCK FOR TRUNK BC TO BLOCKCHAIN P2P NETWORK NODES

Figure 12: MTDPoS figure

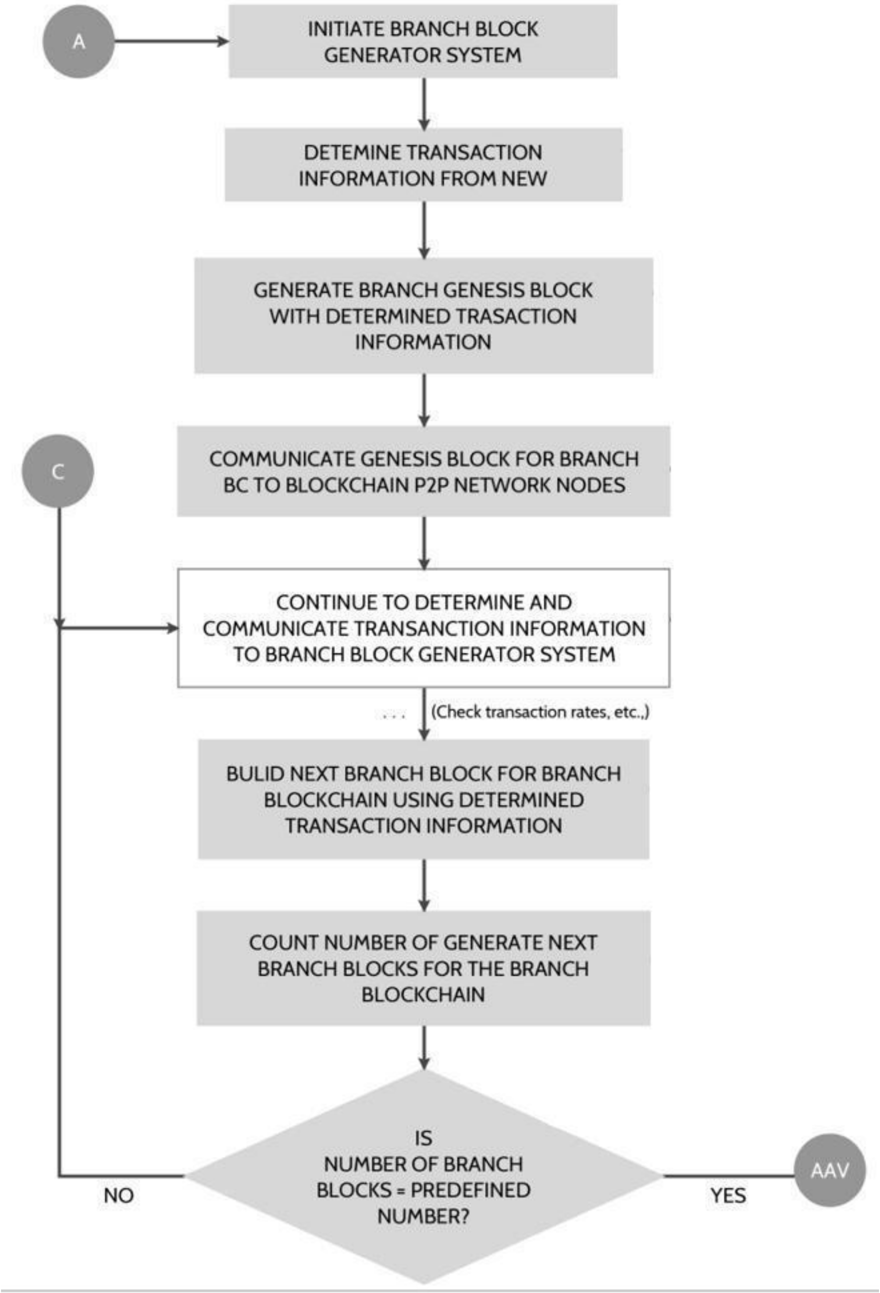

A
INITIATE BRANCH BLOCK GENERATOR SYSTEM
DETEMINE TRANSACTION INFORMATION FROM NEW
GENERATE BRANCH GENESIS BLOCK WITH DETERMINED TRASACTION INFORMATION
C
COMMUNICATE GENESIS BLOCK FOR BRANCH BC TO BLOCKCHAIN P2P NETWORK NODES
CONTINUE TO DETERMINE AND COMMUNICATE TRANSANCTION INFORMATION TO BRANCH BLOCK GENERATOR SYSTEM
. . .
(Check transaction rates, etc.,)
BULID NEXT BRANCH BLOCK FOR BRANCH BLOCKCHAIN USING DETERMINED TRANSACTION INFORMATION
COUNT NUMBER OF GENERATE NEXT BRANCH BLOCKS FOR THE BRANCH BLOCKCHAIN
IS NUMBER OF BRANCH BLOCKS = PREDEFINED NUMBER?
NO
YES
AAV

Figure 13 MTDPoS figure

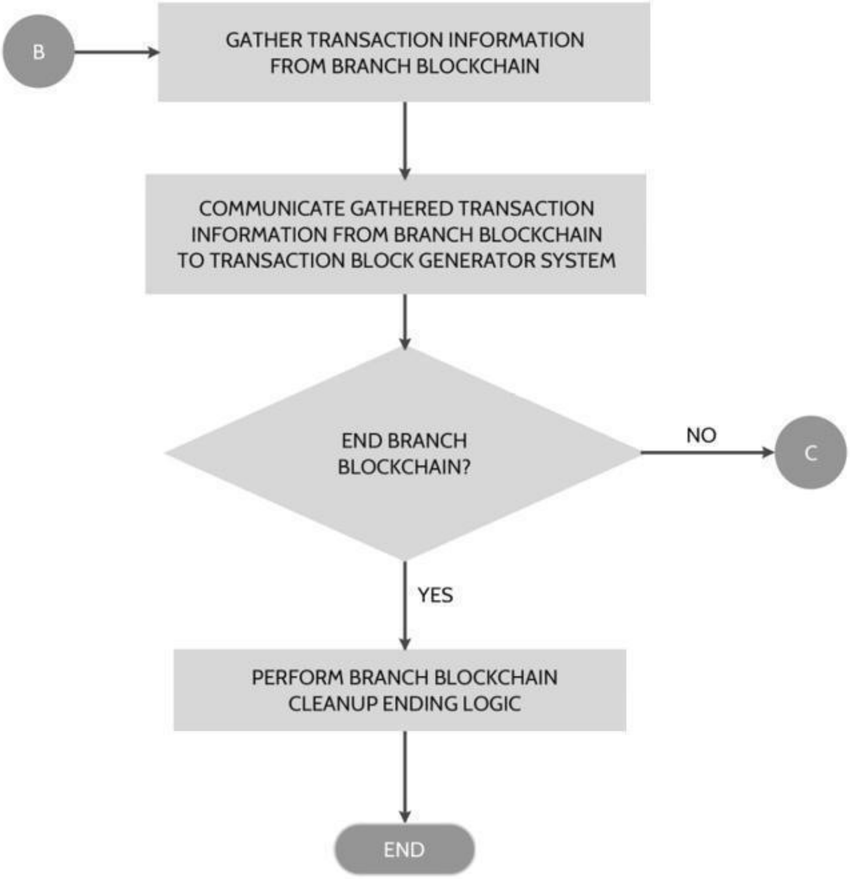

B
GATHER TRANSACTION INFORMATION FROM BRANCH BLOCKCHAIN
COMMUNICATE GATHERED TRANSACTION INFORMATION FROM BRANCH BLOCKCHAIN TO TRANSACTION BLOCK GENERATOR SYSTEM
END BRANCH BLOCKCHAIN?
NO
C
YES
PERFORM BRANCH BLOCKCHAIN CLEANUP ENDING LOGIC
END

Figure 14: MTDPoS

Branch transaction block generator system helps to collect and gather the previous branch block information of Block. After that, the branch transaction block generation passes the collected data to the parent transaction block generator system using Block, for instance, the trunk block generator system. The trunk block generator system processes the communicated information via Block. The gathering process is also called a checkpoint process that collects and remembers the blockchain transaction information.

The Block plays a vital role in deciding whether to end the branch blockchain or not. For instance, the operation of branch blockchain is permitted to complete the transaction. The Block comes into action, thereby cleaning all the logical processes such as releasing the resources, archiving the blockchain information, archiving other crucial details, and ending the blockchain transaction process. If the operation of a branch blockchain is selected to be carried forward, the process goes back to block, and the transactional procedure is continued. For clarification, refer to figure 15.

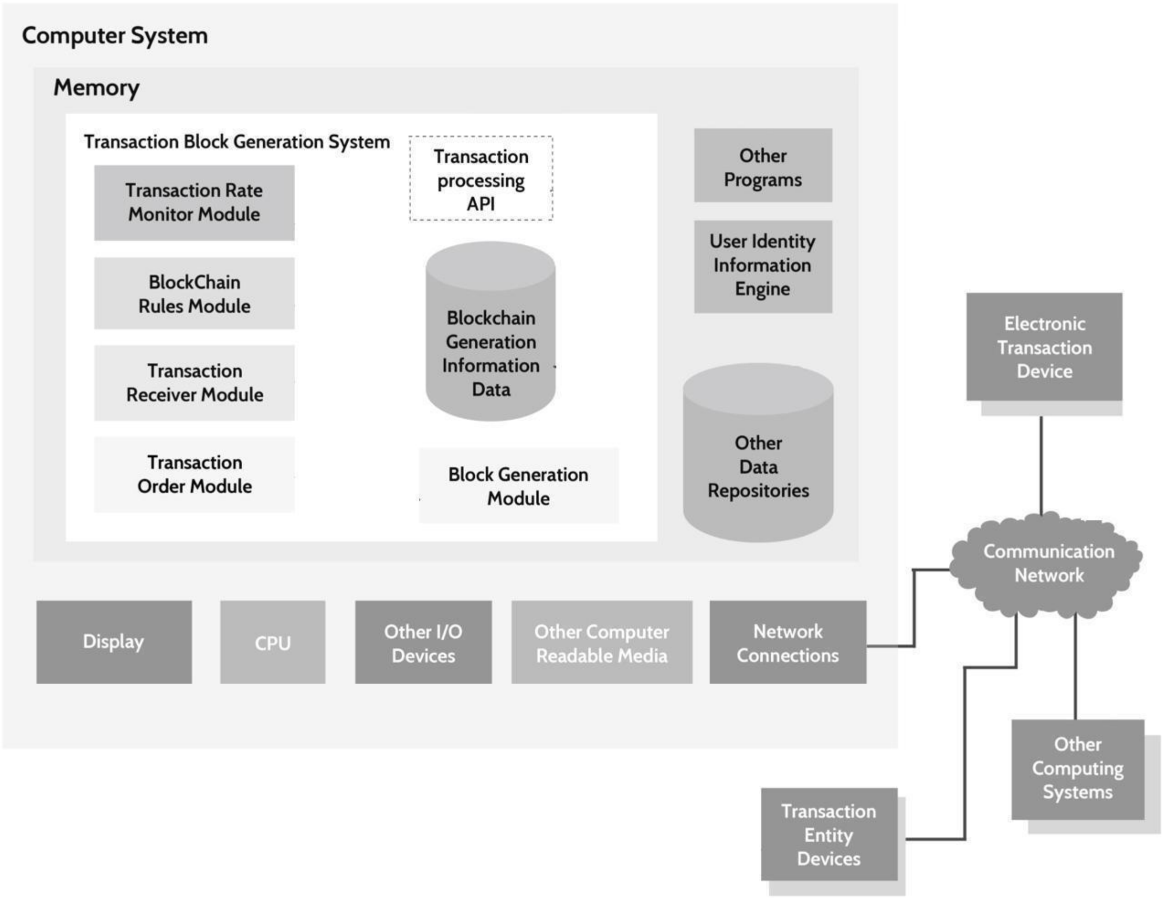

Computer System
Memory
Transaction Block Generation System
Transaction Rate Monitor Module
BlockChain Rules Module
Transaction Receiver Module
Transaction Order Module
Transaction processing API
Blockchain Generation Information Data
Block Generation Module
Other Programs
User Identity Information Engine
Other Data Repositories
Electronic Transaction Device
Communication Network
Display
CPU
Other I/O Devices
Other Computer Readable Media
Network Connections
Other Computing Systems
Transaction Entity Devices

Figure 15: MTDPoS

When there is no transaction information to be prepared and processed, no blocks are generated by the trunk transaction block generator system for the same. The trunk transaction block generator system may generate no block within a predetermined period. Instead, the trunk transaction block generator may create a corresponding block to help communicate the information. There may be instances where the truck transaction block system may not have any additional information to be processed and shared further after receiving the transaction information from the system. This case is referred to as the idle state for the trunk transaction block generator system as it is operating in an inactive state.

Refer to figure 16. This diagram describes the computing system that can be used to incorporate information from the trunk transaction block generator system. The embodiments of the trunk transaction block generator system can be implemented using suitably instructed computing systems, virtual computing systems, physical computing systems or unique computing systems. The trunk transaction block generator system 104 can be executed using individual software, firmware or hardware or can be carried out by a combination of the three. A general-purpose computing system may lack conventional and well-known techniques to carry out the operations required to implement the methods for trunk transaction block generator systems.

A multiuser computing system is helpful as it can be operated by more than one server and client computing system, which is known as a computing system. One advantage that the computing system holds is that the blocks generated can help to represent more than one block and can be combined with other blocks distributed in different locations. This helps to enhance the inter-communication mechanism of the transaction block generator system that uses multiple machines through TCP or IP.

Referring to the embodiment shown in the figure, the computing system consists of the following parts:

- A computer memory.
- A display.
- A Central Processing Units (CPU) may be one or more than one as per the requirement.
- Devices for adding inputs and outputs such as a keyboard, mouse, liquid-crystal display (LCD) and cathode-ray tubes (CRT).
- Other essential computer readable media.
- Network connection may be one or more than one as per the requirement.

The computing memory keeps the transaction block generator system. Depending on the required content, some proportion of the content or all the content can be transferred to the computer-readable media. The transaction block generator system accomplishes and uses one or multiple central processing units (CPUs) to manage the formation of blocks constituting a blockchain. The computing memory also comprises the code of programs and various other data repositories like the data repository, which enhances the execution in the CPUs. Not all the components are required to be present for communication, as shown in Figure 16. To give an idea, not all software may have user input or display.

In a general accepted embodiment, the transaction block generator system consists of:

- One or more than one transaction rate monitor module(s).
- One or more than one blockchain rules module(s).
- One or more than one transaction receiver module(s).
- One or more than one transaction order module(s).
- One or more than one block generation module(s).

In certain embodiments, one or more modules are provided to distribute the communicating network. To illustrate, an external blockchain rules module is provided with the third-party external system to determine and draw the boundaries of the rules of blockchain implementations. The distributed communication network can interact with the transaction block generator system using one or multiple transactions electronic devices, one or more than one transaction entity device. Third-party information would provide computing systems, including purveyors of news used in blockchain generating information data repository. The transaction block generator system can be clubbed with a blockchain generation information data repository to distribute communication. For example, a WWW knowledge base is made accessible to all the communication networks. The blockchain generation information data repository can contain exemplary embodiment, including transactional information, checkpoint information obtained from branches and Metadata information used for generating blocks. The standard programming techniques are used in models and components of the transaction block generator system. For instance, the transaction block generator system can be executed as native implementation running on CPU together with one or more than one dynamic libraries. In another situation, the transaction block generator system can be processed using a virtual machine.

Several programming languages can be used for implementing transaction block generator system information such as object-oriented programming languages (Java, C++, C#, Visual Basic NET and Smalltalk), functional programming languages (ML, Lisp and Scheme), procedural programming languages (Pascal, C, Ada and Modula), scripting programming languages (Perl, Ruby, Python, JavaScript and VBScript) and declarative programming languages (SQL and Prolog).

All the embodiments stated above are known to use proprietary, synchronous, and asynchronous client-server computing techniques. Using executable CPU running on a single computing system or using alternative decomposed variety of structuring techniques having multiprogramming, multithreading, client servers or peer to peer support, running on multiple computer systems can be done by implementing monolithic programming techniques. With the help of message passive techniques, some embodiments implement and communicate the message concurrently and asynchronously. They support synchronous images as well. Using unique components and modules, other functions can be implemented, executed and performed by each component or a module in a different order.

The data stored in the transaction block generator system 104 can be obtained by standard mechanism. These include the following:

- By using C, C++ or Java APIs.
- By utilising libraries used for accessing and reading files.
- By making the use of databases and data repository.
- By using scripting languages such as XML.
- Through Web servers help.
- By using FTP servers.

For storing, combining and implementing the information communicated, the blockchain generation information data repository can be used along with one or more than one database system, file systems and other vital techniques. The embodiments can be stored as procedures or methods attached with the selected items and objects of the transaction block generator system or the blockchain generation information data repository. Other techniques can prove to be equally effective.

The different sets of configurations, locations of programs, and the data are contemplated for use with several techniques described herein. System 104 might be implemented in a distributed environment that comprises several computer systems and networks, even the heterogeneous. Additionally, the server or client may be either physical or virtual computing systems and reside in the same physical system. However, few of the molecules may be distributed, pooled, or grouped, such as balancing load, reliability, or security reasons. Several distributed computing techniques or methods are appropriate for implementing the components of the illustrated embodiments in a distributed manner, including but not limited to the TCP/IP sockets, RPC, RMI, HTTP, Web services (XML-RPC, JAX-RPC, & SOAP) and other such things.

However, in some embodiments, some of the components of the transaction block system 104 might be implemented in some other way, such as at least partially in firmware, but they are not limited to one or more application-specific integrated circuits. Standard integrated circuits, for instance, controllers are executing appropriate instructions, microcontrollers, field-programmable gate arrays and complex programmable logic devices. Some of the system components might also be stored as contents, as executable, machine-readable software instructions, and structured data on a computer-readable medium or other portable media that is to be read by an appropriate driver to enable the computer-readable medium to execute. It could be used as the contents to perform at least some of the described techniques. Some of the components or the data structures might be stored or tangible, non-transitory storage mediums. Some of the system components and the data structures might also be held as data signals on various computer-readable transmission mediums, which are then transmitted across wireless-based and wired based mediums, and might take several forms. Computer program products like that might also take other forms in other embodiments. Accordingly, embodiments of this disclosure might be practised with different types of system configurations.

On the other hand, it should also be emphasised that the above-described embodiments of the transaction tracking system are only possible examples of implementations of the invention. Many other variations and modifications may be made to the described embodiments above. All such changes and the variations are intended to be included herein within the scope of this disclosure and protected by the following claims.

If you can implement and validate the parts or all of the research proposition, that would be great! It would do a strong thesis. Any standard contribution to ETSI PDL would also be an excellent substantial contribution.

9 Architecture core platform

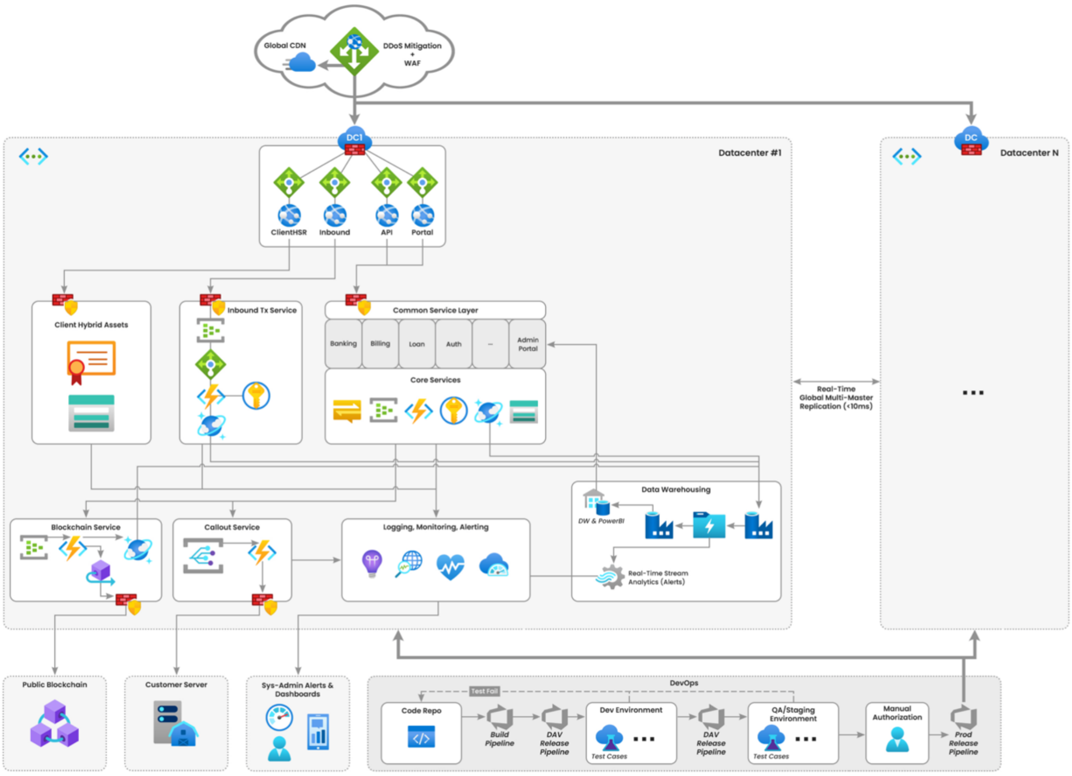


Figure 16: Core MVP

10 Reltime's ecosystem development

This section can be reconstructed and explains different components of Reltime's ecosystem.

Service	Description	Q2 2022 Competed	Q3/Q4 2022 In progress	After 2024
Layer 1 Blockchain	Layer 1 blockchain completed		✓	
	Layer 1 API completed	✓		
	Token facility like CBDC [20]		✓	
	Node validator Programme to be completed in Q3 2022		✓	
SWAP	Swapping crypto allows you to easily exchange one crypto asset for another.	✓		
Bridging	Bridging is the process of transferring coins or tokens from one blockchain network to another. In Reltime Ecosystem we support the following coins or tokens.	✓		
Neobank SaaS	iOS app for App Store to be provided to partners for Whitelabel	✓		
	Android app for Google Play	✓		
	Multi Tenant (create brand to be able to offer a DeFi service)	✓		
	Wallets, with account, joint account, send money for free globally)	✓		
	Landing page	✓		
	Customisations	✓		
Regtech SaaS	Automated KYC onboarding AI	✓		
	Semi-automated KYB onboarding	✓		
	Identity management system, AML/PEP	✓		
	Batch processing system	✓		
DataVault Storage SaaS	Cloud / On-premise storage	✓		
	Multidecentralized (TM) private blockchains network	✓		
	Network management tools	✓		
Biometric login	Passwordless authentication / Face ID / iOS	✓		
	Passwordless authentication / Face Unlock / Android	✓		
	Passwordless authentication / Fingerprint / iOS	✓		
	Passwordless authentication / Fingerprint / Android	✓		
Core-banking system	Administrator control panel for Neobank SaaS	✓		
	Administrator control panel for Regtech SaaS	✓		
	Administrator control panel Datavault Storage SaaS	✓		
	MACP, Master Access Control Panel	✓		
Licences and Certifications coverage	EMI Licence witin the European Economic Area / EEA	✓		
	Alternative Payment Method, 75 checkout	✓		
	Joint account, global coverage	✓		
	PCI DSS Level 1	✓		
	GDPR	✓		

[20] https://azuremarketplace.microsoft.com/nb-no/marketplace/apps/ae8a0ba1-fc8b-4ecc-8599-0fed00daef08.offer_id-07?tab=Overview

	PSD2		✓	
DEX	DEX on top of Reltime Layer 1			✓
Support	Dedicated technical support	✓		
	Dedicated compliance support	✓		
	Dedicated customer support	✓		
Banking-as-a-service	Digital currency support		✓	
	IBAN / ACH issuing for businesses		✓	
	Debit Card issuing / Virtual, Biometric		✓	
	Acquiring	✓		
	Processing	✓		
	White-label card programme		✓	
	Instant International money remittances	✓		
	Reltime and support multi-currency wallets	✓		
	DEFI dApps Lending lending P2P with own terms between B/L	✓		
	Instant peer-to-peer transfers globally	✓		
	Payment GW [21]			✓
	DEX [22]			✓
	DeFi Sandbox OpenAPI to create service for 3party		✓	
	Layer 2 Blockchain with over 300 API [23]			✓
	Decentralised AI [24]			✓
	Reltime, General Ledger		✓	

Table 2: Overview of Reltime's launching plan

This describes the use of funds for this STO/Pre IPO.

10.1 Solution overview

The overall scope comprises developing the following modules to enhance the functionality of the client's existing system.

10.1.1 KYC verification (finalised)

The proposed solution is to develop an AI-enhanced KYC verification platform that uses facial recognition to ensure KYC compliance. The customer will be required to upload their KYC document into the venue. The user will then be required to capture a video of themselves with

[21] https://payment.reltime.com/
[22] https://dex.reltime.com/
[23] https://azuremarketplace.microsoft.com/nb-no/marketplace/apps/ae8a0ba1-fc8b-4ecc-8599-0fed00daef08.offer_id-06?tab=Overview
[24] https://azuremarketplace.microsoft.com/nb-no/marketplace/apps/ae8a0ba1-fc8b-4ecc-8599-0fed00daef08.offer_id-02?tab=Overview

the KYC document in their hand. The system will compare both the user's face and the image in the KYC document. If all the parameters match, then the customer will be able to login into the system.

10.1.2 Crypto lending (finalised)

The proposed application allows the lenders to list the Reltime tokens they own on the platform and receive interest from borrowers. The platform combines blockchain technology and finance. The application enables the borrowers and lenders to conduct the transactions seamlessly.

10.1.3 CRM and General Ledger (finalised)

The system allows the admin to view all the customer log details and their transaction details. The admin will also be able to download all these details. With the aid of the customer relationship management system, the admin will manage all the customers that deal with the client. The admin has the provision to view and import all the data related to customers. The admin can monitor all the customer activities. The solution facilitates the admin to manage the customer database.

10.1.4 MVP App (finalised)

The proposed solution is to develop a mobile application that facilitates the users to perform different crypto-based financial transactions. The solution enables the users to make several payments and transactions through the application. The application will assist the users in making daily crypto transactions at maximum easiness with a mobile phone.

10.2 Onboarding KYC – AI (finalised)

The overall purpose is to deliver with a KYC engine so they can deliver this to the market.

10.2.1 Solutions overview

- Uploaded KYC data (photo images and selfie video) will be processed by stateless APIs provided by Reltime (see below for details)
- Client (ionic/capacitor) plugins will be created to capture photos id's and images (see below for details)
- All server/back-end code will be deployed into an Azure App Service which will expose stateless REST/JSON APIs as defined in "back-end functionality“ below
- Azure BLOB storage will be used for any data storage.

10.2.2 Back-end (Finished)

The back-end will consist of three stateless REST/JSON APIs. They will run in Azure App Service. All information required for these APIs to complete will come from:

- Parameters supplied
- BLOB storage.

i) API #0 - TrainNewID - API for Training new ID type:

1. They are capturing data(Images) along with the Metadata to extract from it. Train each type to enhance what is already done. From Day 1, there is a need for some seed data to train the system and perceive the system. While preparing this model, this data will be reused and introduced again.

2. For example, if a Canadian passport is accepted from day 1, the samples of Canadian passports will be uploaded, and the system will identify the same. The system will automatically detect the passport when the live user comes in and uploads a Canadian passport.

3. API#0 will be used as a data collection API and will not be training independently. The data might need to annotated manually before the training is initiated. This data will be consumed by API #0. This data will be passed on as a JSON file and images annotated based on textual information. The output in this case will be a JSON file.API0.Parameter1:

We would like you to train a path to BLOB storage where there are one or more image examples in the directory of a new ID.

10.2.2.1 API0.Parameter2:

The type of name of this ID can also be stored in *TrainedIDMetadata.json* (see below). If it already exists in *TrainedIDMetadata.json* then old data should be overwritten/replaced for that ID.

This function will:

- Go to the directory in Parameter1, analyse all the files in the manual, and update *TrainedIDMetadata.json* file with whatever information the AI needs to detect this ID in future KYC processes (when API#1 & API#2 below are called).
  Information such as the types of OCR fields extracted, where the photo is located, any other AI/ML data required from training, etc.

- This ID type of name gets put into the *TrainedIDMetadata.json* as the array index will be supplied in Parameter2. If it already exists, then overwrite/replace the data for this ID in the *TrainedIDMetadata.json* file.

The directory of the BLOB storage for training data will be as follows:
<root>/MachineLearningData/TrainedIDMetadata.json - This JSON array contains all the necessary meta-data about each supported ID on the platform. This API updates this file with the new/updated ID metadata after training algorithms to run. The type name of this ID is passed as API0.Parameter2.

<root>/MachineLearningData/<COUNTRY-ISO>/ID001/ - This directory format is used to upload training data for each ID in a country that we support. This path passed as API0.Parameter1.

Examples of what this path could look like:
<root>/MachineLearningData/CA/ID001 - This dir could hold examples of Canadian passports
<root>/MachineLearningData/CA/ID002 - This dir could hold examples of Canadian drivers licenses
<root>/MachineLearningData/NO/ID001 - This dir could hold examples of Norwegian drivers licenses
<root>/MachineLearningData/IN/ID001 - This dir could hold examples of Indian national IDs

10.2.2.2 API0.Response:

JSON indicating if the process was a success or failure. If we fail, then an error code + human-readable reason needs to be returned to identify quickly, correct the issue, and try again.

ii) API #1 - ValidateUploadedID - API for Validating an uploaded Photo-IDAPI1.Parameter1: A path to BLOB storage containing the users uploaded ID

This function will:

- Retrieve the image from API1.Parameter1 and determine which type of ID it is. If it is not in the supported list, return an appropriate error.
- Extract the face image and store it in the exact BLOB location with _facebox appended to the original filename.
- A vector will be generated for a face and will be stored in the DB. When a new photo is uploaded in the system, a vector will be generated for that photo and compared with the vector stored in the DB. The system will create a score for the similarity of the vectors, and if the generated score is above a certain threshold, the system will consider the image to be of the same person. Extract all OCR related data that's supported for this type of ID (as per *TrainedIDMetadat.json*)

The directory of the BLOB storage for the uploaded KYC ID image is as follows:
<root>/KYC/<userid>/<attemptID>/<filename>.jpg - This is where we will upload the image that IONIC/Capacitor plugin captured. This file location will be passed as API1.Parameter1.
<root>/KYC/<userid>/<attemptID>/<filename>_facebox.jpg - This is where this function will place the extracted face image. Note that it is simply _facebox appended to the original input file name in API1.Parameter1.

10.2.2.3 API1.Response:

JSON including the following data:

- The type of ID detected (i.e. the ID type name in *TrainedIDMetadata.json*) and this detection's confidence level (0.0-1.0).
- An array of triplets all the OCR fields. Each array element triplet includes [OCR_FIELD_NAME, OCR_FIELD_VALUE, OCR_FIELD_CONFIDENCE]. Confidence levels are always 0.0-1.0. For example, OCR field names could include name, birthday, gender, document number, expiration date, height, weight, address, etc.

10.2.3 If there are any errors, then an appropriate error code+human readable string must be returned to address the issue and try again.ii) API #2 - ValidateLiveUser - API for Validating an uploaded selfie-video clip of user holding their ID

10.2.3.1 API2.Parameter1:

A path to BLOB storage containing the uploaded video

10.2.3.2 API2.Parameter2:

The face vector of the user, we expect to be in the video (our platform would have received this as one of the response values when we called API1.Response.Image Vector)

This function will:

- -Retrieve the video clip from BLOB storage defined in API2.Parameter1
- Determine if the user is a real live human.
  - The client app will provide instructions to the user to perform specific actions.
  - The AI will determine if it is a live person or not.
- Find the user's face, generate a Vector, and determine the confidence level (0.0-1.0). Then, try several more times again on different video frames to see if a match with a higher confidence level is found.
- Save a video frame with the highest confidence level in the exact BLOB location as the video. However, _facebox should be appended to the file name, and it should be in an image .jpg format.

The directory of the BLOB storage for the uploaded KYC video is as follows. Note that this will reuse the same directory per above:

<root>/KYC/<userid>/<attemptID>/<filename>.mp4 - This is where we will upload the video clip that IONIC/Capacitor plugin captured. This file location will be passed as API2.Parameter1.
<root>/KYC/<userid>/<attemptID>/<filename>_facebox.jpg - This is where this function will place the extracted face image with highest confidence level. Note that it is simply _facebox appended to the original input file name in API2.Parameter2.

10.2.3.3 API2.Response:

JSON including the following data:

- The vector and highest confidence level found in the video that the vector in the video matches the vector supplied in API2.Parameter2.
- If there are any errors, then an appropriate error code+human readable string must be returned to address the issue and try again.

10.2.4 Client front-end

Definitions:
---Calling App
---Plugin - Ionic/Capacitor plugin

- The Plugin will be created for use on iOS and Android.
- The Plugin will be self-contained and only communicate with the calling app.

The calling app will supply several parameters to the plugin during instantiation to be themed to match the calling app, and appropriate instructions can be displayed. The intention is to render a screen similar to Google Pay / Android Pay when taking a credit card picture.

a) General theme/colour scheme information.
b) The approximate size and location of the "camera" window are to be displayed.
c) The instruction text is to display in the area that is not showing the camera/video feed.

- Once the ID is captured, the plugin will do some initial LOCAL (on-device) analysis to ensure the lighting, quality, blur, etc. is acceptable for future AI work on the server. If so, the image will be returned to the calling app. If not, an error will be sent to the calling app to ask the user to try again.
- The calling app will be responsible for transmitting the image to the server middle-tier, at which point API#1 will be called for initial analysis.
- If API#1 is a success, the calling app will be informed, and then the user can proceed to video-selfie analysis.
- The plugin will capture a short video clip instead of an image being captured. All other steps per above will be similar, except the server will call API#2 for live user video validation. Note that the plugin must still do LOCAL (on-device) video analysis to ensure the video clip has sufficient lighting, quality, blurry, etc. The AI on the server can successfully analyse the video clip. Only the minimum length of clip required for successful validation should be returned to the calling app when storing data.

10.3 Reltime's lending (finish)

10.3.1 Solutions overview

- ### Connect wallet
  - The user will be able to connect any of the following wallets:
    - Magic (formerly known as Fortmatic)
    - MetaMask
    - Trust Wallet
- Lending
  - Token listing
    - Users will be able to list the Reltime token on the platform
    - User has to connect their wallet
    - The user can enter the amount of Reltime token that they want to lend
    - The wallet should have the mentioned amount of token
    - The user will be able to set the interest rate for the token
    - The user can set the repayment date
  - Listed token
    - The user will be able to view their listing
    - The user will be able to remove the token from the listing
    - The user will be able to edit their listing
- Borrowing
  - The borrower will be able to view all the listings

    - The borrower will be able to select a listing and can borrow the token
        - The borrower will be required to insert the guarantee fee into the Escrow account
        - The borrower should have the required number of Reltime tokens in the escrow account
    - Once confirmed, the borrower will receive the tokens on their connected wallet
- My borrowings
    - The user will be able to view the active user borrowing
    - The user will be able to view the status of their borrowings
    - The user will be able to repay their borrowings using Reltime tokens
        - After the time period, the Reltime tokens will be withdrawn from the escrow account and will be credited to the lender's account
- Valuation
    - The lender will receive the interest and the capital amount at the end of the predefined period
    - When the valuation goes above the interest rate of the asset
        - The borrower will be able to earn the profit
    - When the valuation goes below the interest rate of the asset
        - The amount is automatically reserved from the escrow account
    - When the valuation goes below 80 per cent of escrow
        - The lender will be able to receive 80 per cent of the loan
        - The borrower will lose 80per cent of the guarantee fee

11 Reltime's PoA Web3 blockchain (example)

11.1 Blockchain - Mainnet

1. Consensus: IBFT 2.0
2. Nodes: 2 Bootnodes, 4 validators (this is basic need for *a whitelabel customer*)
3. Gas fee: 0
4. Block time : 2s
5. Oracle Node
6. Chainlink Node

11.2 Exchange Rebasing

1. Oracle Market Exchange Rate API *: http://api.currencylayer.com/live?access_key=f916e4f4108545f64b5337bd6e76b1d6&currencies=EUR&format=1
2. Number of data providers for CPI rate : 1
3. Number of data providers for Market Exchange Rate : 1
4. Base CPI: 114.50 (Source: https://tradingeconomics.com/euro-area/consumer-price-index-cpi.)
5. Rebase window length : 6 hours
6. Rebase window offset : 1 hour
7. Rebase Interval : 1 Day
8. Rebase Lag : 2

9. Deviation Threshold : 5%
10. Market Rate or CPI Delay : 30 minute
11. Market Rate or CPI Expiration Time : 6 hours
12. If Market Rate or CPI has multiple providers it will take the median of the values from providers.

11.3 Lending and Borrowing

1. Total Amount Calculation: P (1 + rt)
   P : Principal Amount
   R : Annual Interest Rate in PercentageT : Duration in Months
   r = R / 100
   t = T / 12

2. Collateral Calculation:
   (100 + (2 * Interest rate(R))) % of Principal Amount (P)
   P = 500, R = 3%
   Collateral = (100 + (2 x 3)) % of 500
   = 106 % of 500 = 530
   or
   500 + 2 x (500 x 3 / 100) = 500 + 2 x (15) = 500 + 30 = 530
3. Admin Share on each lending: 2% of Principal Amount

11.4 Deliverables

1. IBFT 2.0 Network
2. Explorer
   https://block-explorer-reltime.devtomaster.com/
3. Grafana/Prometheus
4. Chain Link node
5. RTC - Smart contract
6. Digital currency [25] - Smart contract
7. Lending/borrowing marketplace - Smart Contract

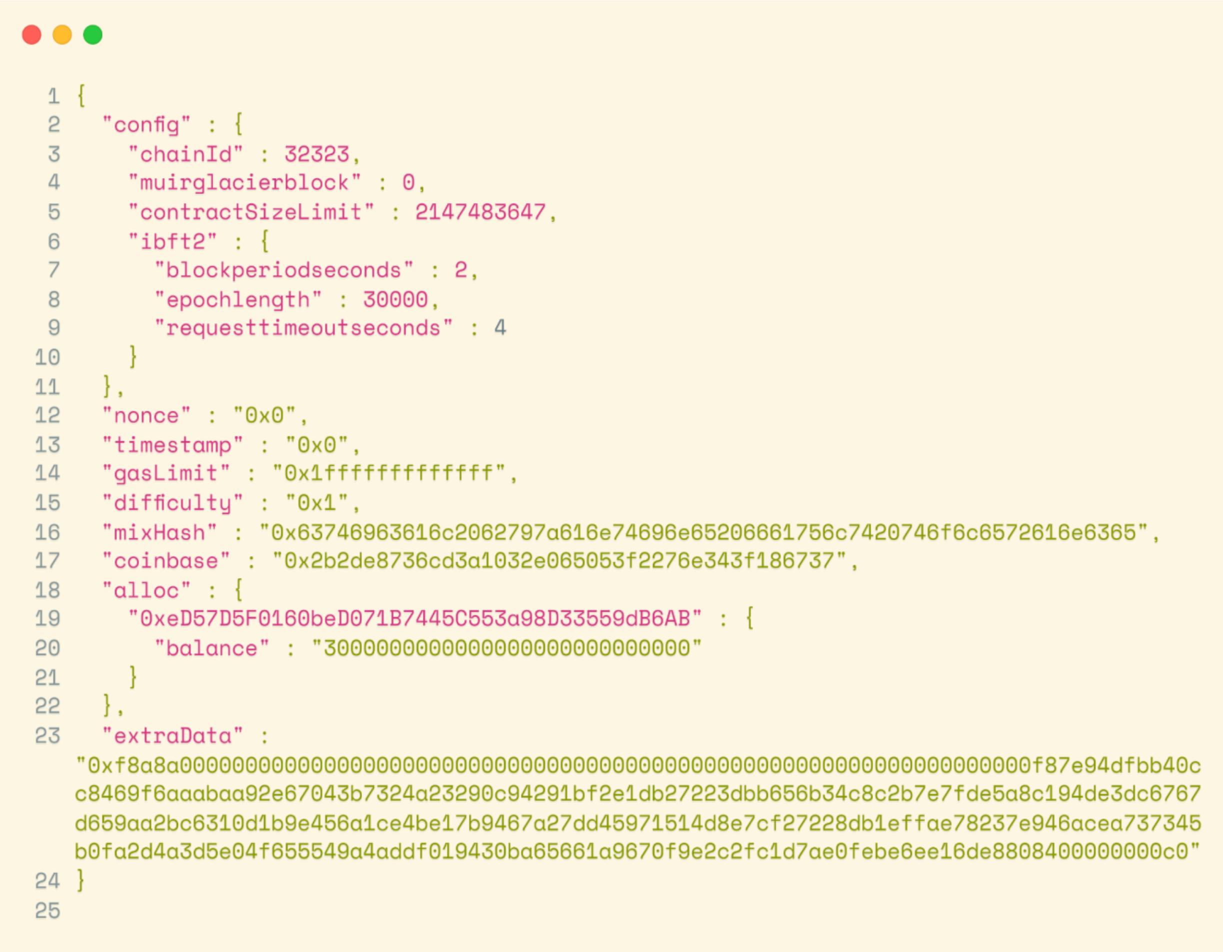
12Reltime's mainnet

12.1 About

Reltime's Mainnet is a *Proof of Authority (PoA)* network with *IBFT 2.0* consensus mechanism. It consists of two bootnodes and four validators . It is a *zero gas network*. More details about the network configuration can be found on the genesis file.

[25] https://azuremarketplace.microsoft.com/en-us/marketplace/apps/ae8a0ba1-fc8b-4ecc-8599-0fed00daef08.offer_id-07?tab=Overview

RPC URL	https://mainnet.reltime.com
SOCKET RPC	wss://mainnet.reltime.com/ws
Chain ID	32323
Block Explorer	https://explorer.reltime.com
Gitlab	https://gitlab.com/r1572/reltime-mainnet/-/tree/development/



```
{
  "config" : {
    "chainId" : 32323,
    "muirglacierblock" : 0,
    "contractSizeLimit" : 2147483647,
    "ibft2" : {
      "blockperiodseconds" : 2,
      "epochlength" : 30000,
      "requesttimeoutseconds" : 4
    }
  },
  "nonce" : "0x0",
  "timestamp" : "0x0",
  "gasLimit" : "0x1fffffffffffff",
  "difficulty" : "0x1",
  "mixHash" : "0x63746963616c2062797a616e74696e65206661756c7420746f6c6572616e6365",
  "coinbase" : "0x2b2de8736cd3a1032e065053f2276e343f186737",
  "alloc" : {
    "0xeD57D5F0160beD071B7445C553a98D33559dB6AB" : {
      "balance" : "3000000000000000000000000000"
    }
  },
  "extraData" :
"0xf8a8a00000000000000000000000000000000000000000000000000000000000000000f87e94dfbb40c
c8469f6aaabaa92e67043b7324a23290c94291bf2e1db27223dbb656b34c8c2b7e7fde5a8c194de3dc6767
d659aa2bc6310d1b9e456a1ce4be17b9467a27dd45971514d8e7cf27228db1effae78237e946acea737345
b0fa2d4a3d5e04f655549a4addf019430ba65661a9670f9e2c2fc1d7ae0febe6ee16de8808400000000c0"
}
```

12.2 Genesis file

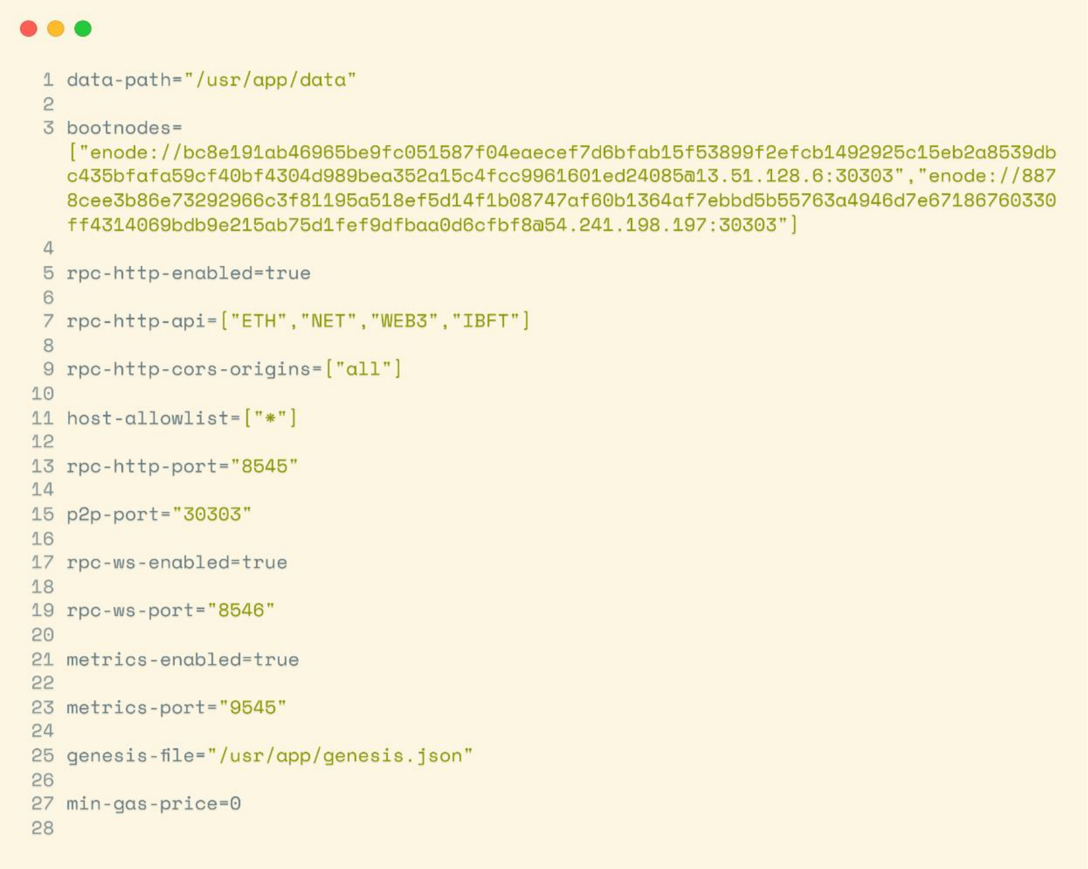
The *Genesis file* (genesis.json) will contain all the details about Reltime Mainnet and the network work according to this. Every node requires a copy of this file inorder to connect to Reltime Mainnet.

12.2.1 Different parameters of genesis file is explained below:

Milestone blocks (Muir Glacier block)	Milestone blocks for the network.
chainID	Chain ID for the network. Random value.
Ibft2	The Specified network uses IBFT 2.0 and contains IBFT 2.0 configuration items.
Blockperiodseconds	The minimum block time is in seconds.
Epochlength	The number of blocks after which to reset all votes.
Requesttimeoutseconds	The timeout for each consensus round before a round. change, in seconds.
coinbase	Address to pay mining rewards to. Can be any value in the genesis block.
gasLimit	Block gas limit. Total gas limit for all transactions in a block.
nonce	Used in block computation. Can be any value in the genesis block.
timestamp	Creation date and time of the block. Must be before the next block so we recommend specifying 0x0 in the genesis file.
alloc	Defines accounts with balances or contracts.
difficulty	IBFT will adjust the difficulty of the network based on hashrate to produce blocks at the targeted frequency.
mixHash	for Istanbul block identification.

12.2.2 Node configuration

The *config.toml* contains all the configuration details about the node. The configuration file must be a valid TOML file composed of key/value pairs. Save the configuration file and restart your node.



```
data-path="/usr/app/data"

bootnodes=
["enode://bc8e191ab46965be9fc051587f04eaecef7d6bfab15f53899f2efcb1492925c15eb2a8539db
c435bfafa59cf40bf4304d989bea352a15c4fcc9961601ed24085a13.51.128.6:30303","enode://887
8cee3b86e73292966c3f81195a518ef5d14f1b08747af60b1364af7ebbd5b55763a4946d7e67186760330
ff4314069bdb9e215ab75d1fef9dfbaa0d6cfbf8a54.241.198.197:30303"]

rpc-http-enabled=true

rpc-http-api=["ETH","NET","WEB3","IBFT"]

rpc-http-cors-origins=["all"]

host-allowlist=["*"]

rpc-http-port="8545"

p2p-port="30303"

rpc-ws-enabled=true

rpc-ws-port="8546"

metrics-enabled=true

metrics-port="9545"

genesis-file="/usr/app/genesis.json"

min-gas-price=0

```

For the bootnode "bootnodes" will not be given. More information on properties can be found here. You can add or remove properties anytime you need and updates will be effective when you restart the node with updated configuration.

12.3 How to run a node

12.3.1 Prerequisites

1. Git
2. Docker and Docker Compose

12.3.2 Steps

1. Clone the repo
2. Make sure the correct genesis file is included in the repo.
3. Configure config.toml according to your node preference
4. Place private and public keys in the '/data' directory (If you already have, otherwise it will be generated automatically).
5. Open a terminal in the folder
6. Run "docker-compose up -d"
7. Node will be running and details can be found on initial logs.

8. Following can be accessed
    - RPC Connection : http://localhost:8545
    - P2P Connection : http://localhost:30303
    - Metrics : http://localhost:9545

All these ports are used by default. If you have configured it in the config.toml change it accordingly.

12.4 How to add a new validator

In an IBFT 2.0 network, add and remove validators by voting.A majority of existing validators must agree to add or remove a validator. That is, more than 50% of validators must execute *ibft_proposeValidatorVote* to add or remove a validator. For example, if you have four validators, the same vote must be made by three validators.

12.4.1 Prerequisites

1. Git
2. Docker and Docker Compose

12.4.2 Steps

1. Setup a new node as per "*How to run a node*".
2. From the initial logs keep the node address.
3. Adding a validator
   Then sent a request with *ibft_proposeValidatorVote*, specifying the address. A majority of validators must execute the call.

   ```
   curl -X POST --data
   '{"jsonrpc":"2.0","method":"ibft_proposeValidatorVote","params":["0xFE3B557E8F
   b62b89F4916B721be55cEb828dBd73", true], "id":1}' <JSON-RPC-endpoint:port>
   ```

   This is an example using curl. You can do the http call using other methods too. When more than half of the existing validators have published a matching proposal, the protocol adds the proposed validator to the validator pool and the validator can begin validating blocks.

4. To return a list of validators and confirm the addition of a proposed validator, use *ibft_getValidatorsByBlockNumber*.

   ```
   curl -X POST --data
   '{"jsonrpc":"2.0","method":"ibft_getValidatorsByBlockNumber","params":["latest"],
   "id":1}' <JSON-RPC-endpoint:port>
   ```

5. To discard your proposal after confirming the addition of a validator, call *ibft_discardValidatorVote*, specifying the address of the proposed validator.

```
curl -X POST --data
'{"jsonrpc":"2.0","method":"ibft_discardValidatorVote","params":["0xFE3B557E8Fb
62b89F4916B721be55cEb828dBd73"], "id":1}' <JSON-RPC-endpoint:port>
```

12.5 Removing a validator

The process for removing a validator from mainnet is the same as adding a validator except you specify *false* as the second parameter of *ibft_proposeValidatorVote*.

12.5.1 Epoch transition

An *epoch transition* occurs in every epochLength block (find epoch on genesis file).
At each epoch transition, testnet discards all pending votes collected from received blocks. Existing proposals remain in effect and validators re-add their vote the next time they create a block.

12.6 Reltime PoA Web3 JavaScript API (finalised)

web3.js is a collection of libraries that allow you to interact with a local or remote node using HTTP, IPC or WebSocket.

The following documentation will guide you through installing and running web3.js as well as providing an API reference documentation with examples.

Keyword Index, Search Page

12.6.1 User documentation

Getting Started
Adding web3.js
Callbacks Promises Events
Glossary
json interface

12.6.2 API Reference

Web3
Web3.modules
Web3 Instance
version
utils
setProvider
providers
givenProvider

BN
isBN
isBigNumber
sha3
sha3Raw
soliditySha3
soliditySha3Raw
isHex
isHexStrict
isAddress
toChecksumAddress
checkAddressChecksum
toHex
stripHexPrefix
toBN
hexToNumberString
hexToNumber
numberToHex
hexToUtf8
hexToAscii
utf8ToHex
asciiToHex
hexToBytes
bytesToHex
toWei
fromWei
unitMap
padLeft
padRight
toTwosComplement

12.6.3 API reference

12.6.4 API

Link

13 Solutions overview

13.1 Language

- The admin will be able to select the language, for example:
  - English
  - German

        - French
        - Italian

13.2 CRM

- Customer management
    - The admin will be able to view all the customer profile
    - The admin will be able to select each customer and view the details of the customer
    - The admin will be able to collect, store and act on data of their customers
    - The admin will be able to view the following data of the customers
        - Document services
        - Product combination
        - Reward points awards and redemption
        - Issued device administration
        - Party data management
        - Customer reference data
        - Location data management
        - Customer relationship management
        - Customer agreement
        - Sales product agreement
        - Customer product/service eligibility
        - Customer precedents
        - Customer proposition
        - Customer event history
        - Party lifecycle management
        - Special pricing conditions
        - Servicing order
        - Customer case management
        - Customer case
        - Card case
        - Customer profile
        - Channel activity history
    - The admin will be able to track the past activities of the customers
- Client interaction tracking
    - The admin will be able to track the interaction activities of the customers
    - The admin will be able to view and track the following activities of the customers
        - Invoices
        - Purchase history
        - Order status

13.3 Marketing automation (new)

13.3.1 Solutions overview

- The admin will be able to send batch E-mails, Web, social and text to the customers
- The admin will be able to create, deliver and track multi-channel marketing campaigns
- The admin will be able to deliver personalised experiences for each customer based on the customer preference and behavioural
- The service domains of the market automation will be:
    - Customer behavioural insights
    - Customer campaign execution
    - Lead/Opportunity management
    - Prospect campaign execution
    - Special pricing conditions
    - Customer campaign management
    - Customer campaign design
    - Prospect campaign management
    - Prospect campaign design

13.4 Regulatory report (finish)

13.4.1 Solution Overview

FUNCTIONAL REQUIREMENTS

- The admin will be able to view all the regulatory reports
    - Legal compliance
    - Regulatory compliance
    - Regulatory reporting
    - Compliance reporting
- The admin will be able to download the regulatory reports
- The admin will be able to submit the regulatory reports to the government officials

13.5 Master Acxcess Control Panel (MACP) access control (completed)

13.5.1 Solutions overview

- The admin will be able to create sub-admins
    - Business direction management
    - Finance and risk management
    - Business development
    - Resource management
- The admin will be able to group the sub-admins
    - Business direction
    - Financial control
    - Operation risk
    - Models and analytics
    - Marketing and development
    - Unit management

- The admin will be able to create the sub-admin credentials
    - Corporate policies
    - Corporate strategy
    - Organisation direction
    - Products and services direction
    - Human resources direction
    - Asset and liability management
    - Financial control
    - Business risk models
    - Operational risk models
    - Production risk models
    - Contribution models
    - Customer behaviour models
    - Credit risk models
    - Fraud models
    - Liquidity risk models
    - Contribution analysis
    - Sales planning
    - Business unit direction
    - Business unit financial analysis
- The admin will be able to set the privileges for the sub admin
- The admin will be able to control the sub admin activities

13.6 Customer support (completed)

13.6.1 Solution overview

- Third-party integration
- The customers will be able to interact with a customer support agent via chat
- The customer support agent will be able to view the messages sent by the customer
- The customer support agent will be able to raise tickets
- The customer will be able to view the status of the raised ticket
- The customer support agent will be able to update the status of the raised ticket

13.7 ERP functionality (in progress)

Solution overview

- Payroll
    - The admin will be able to view the payroll details of all the employees
    - The admin will be able to sort the payroll details based on the dates
    - The admin will be able to view the payroll slip of all the employees
    - The admin will be able to view the account details of the employees
    - The admin will be able to view the transaction details of the employees
    - The admin will be able to block the account of any employee if needed
- Asset ledger
    - The admin will be able to view the log of entries affecting asset accounts from all recorded journal entries

    - The admin will be able to view the details of the debits and credits
    - The admin will be able to view the monthly payment details
    - The admin will be able to view the payment due details

13.8 Reltime App

13.8.1 Solution overview

13.8.2 User module

- Register
    - The user will be required to provide their personal information for registration
    - The user will be required to verify their E-mail ID and mobile number via OTP verification
    - The user will be required to create a password
- KYC verification
    - The users will be able to upload the documents for the KYC verification
        - Third-party integration/ Existing integration
    - The registration will be completed after KYC verification
- Login
    - The users will be able to enter the following information to log in
        - E-mail ID/ Mobile number
        - Password
    - The user will be able to log in using biometric authentication
- Wallets
    - The user will be able to view their wallet details
    - The user will be able to view the list of all the wallets under the user profile
        - The user will be able to select the wallet and can view the transaction details
        - The user will be able to add a new wallet
        - The user will be able to remove the wallet
        - The user will be able to set the default wallet
- Share wallet details
    - The user will be able to select the wallet to which the crypto is to be transferred
    - The user will be able to provide the wallet address
    - The user will be able to share the wallet address through social media
- Send crypto
    - The user will be able to send crypto to another wallet
    - The user will be able to select the crypto in which they want to send the crypto
    - The user will be able to enter the amount of crypto they want to send
    - The user will be able to select the recipient wallet address
        - The user will be able to select the recipient from the contacts
    - The user will be able to add notes if required
    - The user will be able to enter the PIN number to make the transaction
    - After the successful transaction, the user will be able to view the transaction receipt
- Request crypto

    - The user will be able to request crypto from their contacts
    - The user will be able to select the crypto in which they want the crypto
    - The user will be able to enter the amount of crypto they are requesting
    - The user will be able to add the contact information
    - The user will be able to send requests to multiple contacts
    - The user will be able to select the split type
        - Equal split
        - Percentage split
        - Manual split
    - The user will be able to add notes if required
    - The user will be able to enter the PIN number to initiate the request
    - After the request is sent, the user will be able to view the request receipt
- Internal transfer
    - The user will be able to internally transfer the crypto
    - The user will be able to select the type of crypto in which they want to transfer the cryptocurrency
    - The user will be able to enter the amount of crypto they want to transfer
    - The user will be able to select the "From Wallet"
    - The user will be able to select the "To Wallet"
    - The user will be able to add notes if required
    - The user will be able to enter the PIN number to initiate the transfer
    - After the successful transfer of the amount, the user will be able to view the transfer receipt
- Transfer request
    - The user will be able to view all the pending transfer request
    - The user will be able to view the details of the request
        - Requested name
        - Requested crypto
        - Requested date and time
        - Notes if any
    - The user will be able to accept and send the requested amount of crypto
        - The user will be able to edit the details of the request
        - The user will be able to enter the PIN number to initiate the transfer
        - After the successful transaction, the user will be able to view the transaction receipt
    - The user will be able to reject the request
- Transaction history
    - The user will be able to view the details of all the transactions
        - Transaction ID
        - Confirmation ID
        - Contact details
        - Wallet details
        - Date and tme of transaction
        - Transaction amount
- Notification
    - The user will be able to receive the notification of the following
        - Payment request
        - New transactions

      - Payment due dates
    - The user will be able to customise the notification
- Settings
    - Profile
        - The user will be able to view and update the profile details
            - Full name
            - Date of birth
            - Gender
            - E-mail
            - Mobile number
            - Currency
            - Time zone
            - Address
            - Tax information
                - Country of tax residence
                - Tax ID
            - Profile Image
    - Security
        - The user will be able to enable the biometric authentication
        - The user will be able to view the privacy policy
    - Customer support
        - The user will be able to view the customer support mail Id and phone number
        - Third-party integration

14 Platform API Guide

14.1 Document overview

The purpose of this document is to outline the various concepts and API functions available from Reltime's platform.

14.2 Definition

- Reltime customer— Any business entity that has integrated the Reltime Platform into their systems is offering Reltime Services to their End Users.
- End user— The user that will ultimately benefit from the products and services offered by Reltime's platform. End users are not direct customers of Reltime; rather, they are customers of Reltime customers (business customers).
- Reltime's platform—The entire solution that's described in this document.
- Solution overview

14.3 General API overview

Reltime's platform provides two types of APIs, Public API and Administrative API. Public API contains a set of APIs that are executed on behalf of an End User. Public API is used to provide Reltime's services (e.g. banking, microloans, credit cards, etc.) to End Users. Administrative API contains a set of APIs that are used by Reltime's customers to monitor and sync the data in Reltime's platform. Furthermore, Administrative API can be used to retrieve a Public API token for an End User so that Reltime's customer can send requests on behalf of the End User to Public API.

This section explains the API design principles that are shared between Public API and Administrative API. Please see the following sections for the information specific to each API.

Reltime APIs use the REST protocol. This means that an API function can be invoked by simply sending a HTTP request to the API URL. However, the following needs to be taken into consideration when sending requests to the APIs.

14.3.1 Reltime's services

Reltime's platform consists of multiple Services. Each service has its own API endpoint suffix, E2EE endpoint and is separately versioned. The table below shows the list of Reltime's services.

Service name	Description
Security	This service handles user authentications and registrations. This service is only used in Reltime's Public API.

Platform	This service includes the fundamental platform services shared among all other Services.
Banking	This service includes a high-performance accounting engine and financial account services.
Billing	This service includes a flexible billing engine that generates invoices and tracks charges to Reltime's customers. This service is only used in Reltime's Administrative API.
Loan	This service includes the services related to the micro-loan marketplace that connects lenders to end users.
Blockchain	This service includes a blockchain service that securely stores a receipt/confirmation of a transaction on one or more blockchains.

14.3.2 Security

14.3.2.1 Custom URL

A custom API URL will be generated for each Reltime customer and API type pair. Administrative API and Public API will use different API URLs. The provided URL must be used to send requests to the API. Otherwise, a 401 HTTP status code will be returned.

14.3.2.2 End-to-end encryption (E2EE)

All requests need to be end-to-end encrypted using a hybrid encryption scheme. See the Reltime Security and E2EE Details document for the detailed steps to encrypt the request and decrypt the response. Note that different sets of E2EE server certificates are used for Administrative API and Public API. See Appendix A. Sample Request and Response for E2EE JSON and HTTP request/response samples.

Reltime APIs expose a single secure E2EE endpoint for each Service in the API which accepts all requests for the API endpoints within the Service. The client encloses the HTTP request details (URL path, query strings, headers, body, etc.) in a JSON object, encrypts the JSON object and sends the encrypted JSON object to the secure endpoint for the Service. Then, the secure endpoint decrypts the request, internally forwards the decrypted request to the requested endpoint and returns the encrypted response. Please see 3.2.1. E2EE Endpoint URL for Public API secure endpoint URLs and 4.1.1. E2EE EndpointURL for Administrative API secure endpoint URLs.

14.3.3 Error handling

14.3.3.1 Client provided request GUID

The client should create a unique ID for each request (request GUID) and include it in all REL—REQ-ID HTTP header requests. This value should also be included in all Reltime support requests.

14.3.3.1.1 HTTP status codes

Reltime APIs return three different error HTTP status codes.

14.3.3.1.2 400 Bad request

This status code indicates that the error resulted from the user input. The client should validate the input before sending the request again.

14.3.3.1.3 500 Internal server error

This status code indicates that the error occurred inside the Reltime API. If this error persists, please report to Reltime’s technical support team with the returned traceId and request GUID of the request.

14.3.3.1.4 401 Unauthorised

This status code indicates that the provided credentials are not valid. The client should ask for a different mobile number or authentication code for the Public API and check the API key and secret for the Administrative API. The response body for this status code is empty.

14.3.3.2 Error response elements

Reltime APIs return a JSON object containing the following fields based on RFC 7807-Problem Details for HTTP APIs.

14.3.4 Versioning

Reltime APIs use versioning to ensure backward compatibility. When an API undergoes a significant change that is not backward compatible, the API update will be released as a new version. The old version of the API will still be supported, while customers migrate to the new version. Clients will be notified in advance before old versions of the API are deprecated and removed.

14.3.4.1 Version location

API version is included in the API URL. Please see 3.2. URL Scheme for Public API and Administrative API. For Public API, each service is separately versioned.

14.4 Public API (several finalised)

14.4.1 This section explains the details specific to the Public API, which is used to execute operations on behalf of an end user.

14.4.2 URL scheme

All Public API endpoint URLs follow the format:

URL element	Definition
<Custom URL>	Custom Public API URL for Reltime's customer. Reltime API uses custom URLs for security purposes. See 2.2.1. Custom URL for details.
<Reltime ServiceName>	Name of Reltime's service in lowercase
<Version>	API version ex) v1, v2, …
<Endpoint Address>	URL specific to each API endpoint. See Swagger Documentation for the address of each API endpoint.

14.4.3 Token-based authentication

Unless otherwise specified, all endpoints in Public API require a token. To do so, include a token in the HTTP header as below.

Location:	Authorization HTTP Header
Format:	Authorization: <Scheme> <Credentials>
Scheme:	Bearer
Credentials:	Token (JSON Web Signature Object)

14.4.3.1 Device bound tokens

The token is bound to the device it was issued to. All requests should include the client hardware ID of the client device in the REL-CLIENT-HARDWARE-ID HTTP header. This value is matched against the client hardware ID provided to the endpoint when the token was first created. If the values do not match, a 401 Unauthorized response is returned.

14.4.3.2 Token signature verification

When receiving a token, the client should verify its signature. The token is a JSON Web Signature object. The payload is signed using RS256 with the E2EE server integrity certificate. The client should verify the signature using the certificate's public key.

14.4.3.3 Retrieving a token

A new token can be retrieved from /Auth/* endpoints in Security Service through the SMS authentication method using an end user's registered mobile number.

14.4.4 Swagger documentation

The following URL contains the Swagger UI documentation for endpoints in Reltime's services.

14.5 Administrative API

This section explains the details specific to the Administrative API, which is used to monitor and sync the data in Reltime's platform.

14.5.1 URL scheme

All Administrative API endpoint URLs follow the format:

URL element	Definition
<Custom URL>	Custom Administrative API URL for Reltime's customer. Reltime API uses custom. URLs for security purposes. See 2.2.1. Custom URL for details.
<Reltime ServiceName>	Name of Reltime's service in lowercase
<Version>	API version ex) v1, v2, …
<Endpoint Address>	URL specific to each API endpoint. See Swagger Documentation for the address of each API endpoint.

14.5.1.1 E2EE endpoint URL

Each Reltime Service has its E2EE endpoint. All E2EE endpoint URLs follow the URL scheme above and use the <Endpoint Address>.

14.5.2 Common HTTP request elements

14.5.2.1 E2EE request headers

The following HTTP elements should be included in the E2EE request (not inside the E2EE request body).

14.5.2.2 Inner request HTTP elements

The HTTP elements should be included in the inner request inside the E2EE request body.

14.5.3 API Key authentication

All endpoints in Administrative API require an API key and secret specific to a Reltime customer. Include the credentials in the HTTP header below.

Location: Authorization HTTP Header
Format: Authorization: <Scheme> <Credentials>
Scheme: Basic
Credentials: Base64 encoded string created by the steps below.

1. Concatenate the API key, a single colon (":") character and the API secret.
2. Encode the concatenated string into a byte array using UTF-8 encoding.

14.5.4 Callback notifications

Administrative API notifies a Reltime customer of events in Reltime's platform by sending an HTTP POST request to a pre-configured URL. A Reltime customer can choose a list of events for which to receive notifications. See Appendix B. Callback notification types and payloads for the complete list of notification event types.

Retry mechanism

Reltime's platform re-sends the notification to the pre-configured URL if the endpoint does not respond in time or returns a status code other than exceeding 200.

14.5.4.1 Callback request elements

14.5.4.1.1 callbackId

Description: Reltime generated a unique identifier for this
callback event. Data Type: String

Required: Yes

14.5.5 Swagger documentation

The following URL contains the Swagger UI documentation for endpoints in all
Reltime Services.
https://<Custom URL>/swagger.

Appendix B. Callback notification types and payloads

This section contains the list of different callback payload types. It also includes the list of callback notification types that use the callback payload type and the list of additional callback request elements the callback payload contains and callback request elements.

14.5.6 End user auth code payload

14.5.6.1 Callback notification types

Notification type	Description
END_USER_AUTH_CODE	Triggered when an end user authentication code is sent from Administrative API.

14.5.7 End user payload

14.5.7.1 Callback notification types

Notification type	Description
END_USER_ADDED	Triggered when a new end user is added.
END_USER_ACCEPTED_REQUIRED_POLICY	Triggered when an end user accepts a required policy.
END_USER_UPDATED_STATUS	Triggered when an end user status gets changed.
END_USER_UPDATED_OTHER	Triggered when other end user details get updated.

14.5.7.2 Additional callback request elements

14.5.7.2.1 endUserId

Description: Unique identifier of the end
user Data Type: String
Required: Yes

Account payload

14.5.7.3 Callback notification types

Notification type	Description
ACCOUNT_VIRTUAL_BANK_CREATED	Triggered when a new virtual bank account is created.
ACCOUNT_LOAN_CREATED	Triggered when a new loan account is created.
ACCOUNT_UPDATED_STATUS	Triggered when an account status gets changed.
ACCOUNT_UPDATED_AUTO_PAYMENT	Triggered when an account's auto payment details are updated
ACCOUNT_UPDATED_OTHER	Triggered when other account details are updated

*Note: Creating a new credit card triggers a CREDIT_CARD_APPLICATION_CREATED event.

14.5.8 Transaction payload

14.5.8.1 Callback notification types

Notification type	Description
ACCOUNT_TRANSACTION_CREATED	Triggered when a transaction is created.
ACCOUNT_TRANSACTION_UPDATED	Triggered when a transaction is updated.

14.5.9 Money request payload

14.5.9.1 Callback notification types

Notification type	Description
MONEY_REQUEST_CREATED	Triggered when a money request is created.
MONEY_REQUEST_UPDATED	Triggered when a money request is updated.

14.5.10 Account statement payload

14.5.10.1 Callback notification types

Notification type	Description
ACCOUNT_LOAN_STATEMENT_CREATED	Triggered when a loan statement is created.
ACCOUNT_CREDIT_CARD_STATEMENT_CREATED	Triggered when a credit card statement is created.

14.5.11 Credit card application payload

14.5.11.1 Callback notification types

Notification type	Description
CREDIT_CARD_APPLICATION_CREATED	Triggered when a new credit card application is created.
CREDIT_CARD_APPLICATION_UPDATED	Triggered when a credit card application is updated.

14.5.12 Tenant payload

14.5.12.1 Callback notification types

Notification type	Description
TENANT_DETAILS_UPDATED	Triggered when a tenant's details get updated.
TENANT_CONFIG_WLASSET_CHANGED	Triggered when the tenant white-label asset gets changed.
TENANT_CONFIG_API_CHANGED	Triggered when public API configuration gets changed.
TENANT_MOBILE_VERLIST_CHANGED	Triggered when the list of allowed mobile client versions gets changed.
TENANT_MOBILE_FIRST_SCREEN_CHANGED	Triggered when the mobile first screen gets updated.
TENANT_REQUIRED_POLICIES_CHANGED	Triggered when required policies get updated.
TENANT_TIP_CHANGED	Triggered when mobile tip gets updated.

14.5.12.2 Additional callback request elements

This payload does not have any additional request elements.

14.5.13 Tenant transaction payload

14.5.13.1 Callback notification types

Notification type	Description
TENANT_BILLING_TRANSACTION_CREATED	Triggered when a billing transaction is created.
TENANT_BILLING_TRANSACTION_UPDATED	Triggered when a billing transaction is updated.

14.5.14 Tenant invoice payload

14.5.14.1 Callback notification types

Notification type	Description
TENANT_INVOICE_CREATED	Triggered when a new invoice is created.

15Reference

15.1 Press Release

Here is the press releaseas: https://www.reltime.com/press-releases
Media and News: https://www.reltime.com/reltime-in-media

15.2 Decentralised Science

Decentralised Sience, where we develop new project like Decentralised AI and utilising the mobile handset as Node. https://www.reltime.com/desci
Handset: https://computerresearch.org/index.php/computer/article/view/102332
Award: https://news.cision.com/reltime-as/r/frode-van-der-laak-wins--best-researcher-award--from-the-international-congress-for-research-excelle,c3933686

Figure 17: Reltime won the best AI and Web3 [26]

[26] https://news.cision.com/reltime-as/r/reltime-receives-prestigious-nordic-innovation-award-for--best-ai---web3-fintech-of-2023-,c3776594