Part 2:
The TǫrǫNet Infrastructure

Making the promise of a better future, enabled by blockchain infrastructure, a reality for millions.

Yellow Paper

Table of Contents

TọrọNet Project Papers

The project papers are in 3 parts. The white paper, which presents a description of the TọrọNet Project is part 1 of 3 papers; Part 2 {the Yellow paper} describe the technical features of the underlying blockchain infrastructure (TọrọNet Chain), network and ecosystem; and , Part 3 { the Green paper} describes the governance and administration of the ecosystem

This Document is not a Prospectus.

These 3 documents does not constitute nor imply a prospectus of any sort. No wording contained herein should be construed as a solicitation for investment. Accordingly, this whitepaper does not pertain in any way to an offering of securities in any jurisdiction worldwide whatsoever. Rather, this whitepaper constitutes a technical description of the functionality of the **TọrọNet** chain.

This Document is not a final design specification

These documents does not constitute nor imply a final design specification of **TọrọNet** project, technology and governance arrangements .. Information presented on these papers, technical or otherwise, is meant to outline the general idea of TọrọNet project, its design and its use-cases and is subject to change with or without notice. For the latest up-to-date technical specification, check out the updates and documentations on the testnet explorer https://testnet.toronet.org/ or the mainnet explorer at https://toronet.org/explorer/

Part 2

The TờrộNet Chain

2.0 Detailed Description of the TọrọNet Chain Infrastructure

The technical details of **the TọrọNet** blockchain implementation are discussed in this section.

These are described in this section.

2.1 The TọrọNet Blockchain Formulation

The TọrọNet blockchain is a ledger consisting of accounts and balances. The code base was initially set up from the Ethereum code, and then subsequently developed to add the desired features described in solution section, and replacing certain features including the fee system, and proof of work consensus algorithm. However, the network retains the smart contract language syntax, as well as the cryptographic and hashing function from the Ethereum network. The resulting technical formulation for this network is described in this section.

2.2 TọrọNet Consensus Process

The TọrọNet consensus process is a proof of authority consensus model and is a modification of proof of proof of work and proof of stake algorithms. In this process, only trusted participants are accepted in the network. Transaction processing nodes are all trusted and approved nodes with significant deposits or stake in the reserves. The POW difficulty algorithm is set so low such that any participant is able create blocks. However, the algorithm limits the total transaction value that can be mined by any node within a span of time (set to about two weeks) to be no greater than the value the node operator has invested in reserve (staked value.) Using this model, node operator can be trusted to produce blocks without requiring them to run expensive calculations and wasting electricity and computing resources. Their staked value provides the trust necessary for the blocks generated. The blocks do still have to be computed using a POW algorithm and are still chained to all prior blocks in history by cryptographic algorithm built into the blockchain.

As a result of these changes, the difficulty level required to create a block is set really low for the TọrọNet network, and blocks are created every 2 seconds. **Thus, it takes between 2 and 3 seconds to confirm a transaction on the TọrọNet blockchain.**

2.3 No Minting Rewards to Miners

Another key modification in the current definition compared with other blockchains, including the Ethereum blockchain is that the writing of a block does not result in minting of new value, or reward to the transaction processor, also known as the miner. So how are transactions paid for? Every transaction carries a transaction fee. The method of rewarding processing nodes with new mint, we feel is economically distortive. It might initially create an illusion of cheaper transaction costs, but that cost is simply taken from the system, and other users of the currency, in providing the rewards for growth in

the system to transaction processors when actually the activity being performed is a service rather than a creative process.

2.4 Creative and Transformative Transactions

For simplicity, we identify two types of transactions in a theoretically isolated economic sub-domain. Those which transfer value among members of the ecosystem and those that result in completely new value that hitherto never existed in the system. In the TǫrǫNet eco-system the transactions that are creative and results in new mint include the following:

1. Deposit of fiat currency into the reserve. This results in the creation of an equivalent amount of Tǫrǫs at the current exchange rate.
2. Deposit of fiat currency into the reserve to create a collateral or to lend on the network.
3. Deposit of fiat currency or other cryptocurrency such as Ethereum that automatically results in minting of new Tǫrǫs of equivalent value.

3.0 Smart Contracts and Operations of the TǫrǫNet Chain

TǫrǫNet uses smart contracts to manage all assets on the blockchain. The tokens created on the blockchains are themselves created by smart contracts such that the fee structure is not on the blockchain layer and are thus part of the operational purview of the Association. This section describes these smart contracts including those used for setting up and operating savings, loan contracts, collateral contracts, as well as how the operational modus operandi is set up using game theory to create the offchain and onchain incentives to ensure contract fulfilment.

3.1 How the Native Tokens Tǫrǫ are created in the network

The following are the fundamental principles behind asset creation, tokens, and contracts on the network:

Categories of assets and how they are Created on TǫrǫChain

Tǫrǫs are created in the following ways:

1. Anyone can deposit equivalent fiat in offchain reserves or cryptocurrency into Tǫrǫ cryptocurrency reserve, and have equivalent stablecoin of the same value created on the Tǫrǫ blockchain.
2. Stablecoins can be converted to Tǫrǫs .
3. Smart contract derivative Tǫrǫs are created and can convert to Tǫrǫs
4. Assets that are secured by the blockchain are tokenized . These are non-fungible tokens (NFTs).
5. Tokenized collaterals or virtual assets can be created from values deposited into the reserves or staked Tǫrǫs.

3.2 Fiat-to-Chain and Cross-chain Mechanism

TǫrǫNet uses tokens to bring in external tokens to TǫrǫNet in a trustless manner and allow trustless financial contracts and trading of all major cryptoasset tokens.

The token standards are similar to ERC20 on Ethereum and Omni on Bitcoin blockchain. Through this standard, TǫrǫNetChain allows tokenization of any asset including fiat currencies and cryptocurrencies.

All tokens created on the network are asset-backed tokens created with the backing of cryptoassets or fiat currencies. For instance, if a user on the network deposits USD 100 in the system, the amount is placed in the TǫrǫNet offchain reserve, and an equivalent amount in stablecoin USD is credited to the user's account on the blockchain. Further, if the user deposits the stablecoin USD in blockchain reserve, an equivalent amount in Tǫrǫs is minted and deposited in the user's account on the blockchain. The rate of conversion between the stablecoins and the native Tǫrǫs are set by oracles maintained by the network utilizing several public exchange rate benchmarks. The rates as set such that tokenizing an asset on the blockchain is usually 1:1.

3.3 Savings Contract in the TǫrǫNet Ecosystem

A monetary ecosystem is incomplete without a savings strategy within the system. Savers provide liquidity within the system for enterprising entities; in this case users seeking to purchase assets such as smartphones, vehicles, houses, or even farmers seeking development loans.

The system would need to provide some incentive for savings. This does require some balance as well. A system where savings are too incentivized typically results in one where many hold and do not spend their resources and the economic system does not grow.

Several blockchains have introduced the concept of savings by allowing account owners to stake (lock) balances in their wallet for some length of time in exchange for some of the new mining rewards. An example is the Dash network.[9] And some blockchains are almost completely investment mechanisms because they are so deflationary that their value keeps rising and significant enterprise or spending as a ratio of the circulation remains low; for example, bitcoins.

In TǫrǫNet, we introduce a completely new way of accommodating those who wish to save their assets while incentivizing them to do so. The savings is discounted off the reserve such that the association, the administrative node has room off the reserve to make loans or microloans to users in the ecosystem via network members that results in growth to the reserve on repayment with interest.

To accomplish this, we designed a contract asset, TǫrǫSV, which has the same conversion rate and value as Tǫrǫs. However, bearers of this asset receive back a proportion of the overall growth of the reserve. If the reserves do not grow, they have no reward. To convert a Tǫrǫs to TǫrǫSV, a user simply needs to send their Tǫrǫs to the reserve and an equivalent amount of TǫrǫSV is deposited into their account.

3.4 Loan Contract

Loan Contract is designed to allow the owner of the contract to take a collateralized loan against collateral locked in the contract. Each loan contract is unique to every owner (address) on TǫrǫNetChain.

Any user can open a loan contract on TǫrǫNetChain. The user who opens a loan contract owns the specific contract. This ownership, however, is transferable.

Once a loan contract is opened, it may be funded with Tǫrǫs or any stablecoin on the blockchain. Once a loan contract is funded, it allows the owner to take out a loan by minting derivative loan Tǫrǫs. (It should be noted that the loaner's funds could come from a combination of traded collaterals. This process is described in Section 3.5.) It should be noted that in this and other cases, the Tòrònet

association and the network in general provides this smart contract templates as an infrastructure. Independent nodes on the platform are expected to utilize these smart contracts to develop these into services in the various communities using the network.

3.5 Tradeable Collateral Contracts

TọrọNet also introduces tradeable collaterals in a smart contract template expected to be utilized by nodes in the ecosystem. This is a new concept brought to the blockchain space on the realization that a lot of times liquidity can frequently exist in different geographical locations by country. In such situations, owners of such resources would like to benefit from returns that could accrue from putting such resources to work in form of making loans in the locations where they are needed. However, there currently exists no procedure to allow this to occur without risking those resources due to lack of an ability to perform due diligence on borrowers or monitor performance or enforce the terms of the loans.

A tradeable collateral contract allows the resource to be collaterized on the blockchain in its own jurisdiction, and the power of the collateral traded to a member of the blockchain in the local jurisdiction, who has the local knowledge, access, and proximity to borrowers and able to process such loans. The eventual tradeable contract is structured such that the operator has no means of monetizing the collateral besides the successful performance of the loans, and is incentivized to receive rewards only on performance. The operator also is required to stake other resources to guarantee the loan activity. Finally, the local collateral on the loan is still retained in the form of tokenized asset as described in Section 3.5 – including deeds, auto, or smart phone registration to which the blockchain Association retains rights until the terms of the loans are satisfied.

3.5.1 Bundling of Collaterals

Traded collaterals are typically expected to be bundled in a composite such that a collateral exposure is not to one loan, but is secured by several loan contracts. The reverse is also the case. This is illustrated in Figure 1. This is a risk management feature built into the collaterals and loans contract.

3.5.2 Security for Lender, Borrower, and Tòrònet

The TọrọNet platform Defi formulation utilizes the advantages of blockchain smart contracts to manage a loan and enforce loan terms. Unlike most DEFI projects, Toronet loan collaterals are expected to be used for real world items such as mortgaged homes, car loans, and loans for smart phones, which facilitate business opportunities. The loans payments are made directly to an operator or dealer by utilizing a special type of Tọrọs provided to the borrower. The special Tọrọs can only be cashed by such dealers. Secondly, the dealer who is also a user registered to that role on the blockchain is required to register in the real world to the node. This is critical since the node is the actual entity providing the funds guarantee from it's reserves.

Similar to crowd funding structure, multiple funding sources can be aggregated using a system of tradeable collaterals. In the event of a default on the blockchain, in the real world the dealer is then able to reclaim the collateral. The dealer rewards are built into the smart contract. Similar to secured loans on real world assets in traditional finance, insurance is required for items that are secured by loans throughout the duration of the loans; to ensure that the no significant part of off-chain operations resolves into debt collection activities. The loan administration cost for this arrangement is the rewards allocated to dealers and the insurance cost of the secured items, and is expected to be lower than for traditional finance. However, it is expected that nodes on TòrọNet platform will also still able to make blockchain loans to real people in communities with real finance needs.

3.7 Transparency of the Reserve

The balances of all currencies in the reserve will be published on the TòrọNet public blockchain website or explorer. The values in the reserve will be maintained in reputable banking institution so that it would be verifiable that indeed the issued currencies are backed by the reserves that are intended to cover their liquidity. It should be noted, that it is implied, and expected that the Administrative nodes could withdraw to cover operational costs of running the network from the reserves up to the reserve margin. All such withdrawals will also be on the blockchain and can be viewed publicly.

3.8 Decentralized Exchange (DEX)

The TòrọNet ecosystem includes a decentralized exchange within the network. Several assets can be traded or exchanged for each other based on the exchange rate determined by oracles within the blockchain. The exchange allows trading (exchange) of several assets including fiat currencies in operating communities, Tòrọs, derived Tòrọs, and several cryptocurrencies including Bitcoin and Ethereum.

Table 1. Exchange Rates for Different Types of Asset Exchanges on the Network

Asset	Exchange Type	StableCoin of Fiat	Exchange Rate
Local Fiat Currency eg. Cedi, Naira, Kenyan Shillings, etc.	Fiat Currency to Stablecoin Fiat Token on Blockchain	Tokenized Local Currency or Stablecoin	1.1:1 conversion to stablecoin
Stablecoin or Tokenized Local Fiat Currency	Stablecoin Fiat Token back to Fiat Currency for Withdrawal	Local Fiat Currency	2. 1: (1 - *x*) *x* is a small margin such as 0.02
Stablecoin	Stablecoin to Tòrọ	Tòrọ	3. Rate set by Blockchain oracle
Cryptocurrency eg. Bitcoin, Ethereum	Cryptocurrency to Tokenized Cryptocurrency	Tokenized Cryptocurrency	4.1:1 conversion to tokenized cryptocurrency
Tokenized Cryptocurrency	Tokenized Cryptocurrency to Cryptocurrency	Cryptocurrency eg. Bitcoin, Ethereum	5. 1: (1 - *x*) *x* is a small margin such as 0.02

Derived Stablecoin	Derived stablecoin to Stablecoin	Stablecoin	6. 1: (1 – *y*) *y* is a small margin such as 0.0
Stablecoin	Stablecoin to Derived Stablecoin	Stablecoin	7. 1:1

TǫrǫNet will support local currencies in each jurisdiction of operation (Figure 1.) as well as cryptocurrencies. At the start, Bitcoin and Ethereum will likely be supported. Other cryptocurrencies may be added later as decided by the Association. Each supported asset will have its own reserve account to maintain backing for the tokenized asset on the blockchain. The balance of each reserve will be transparent and verifiable on the blockchain as shown in Figure 1.

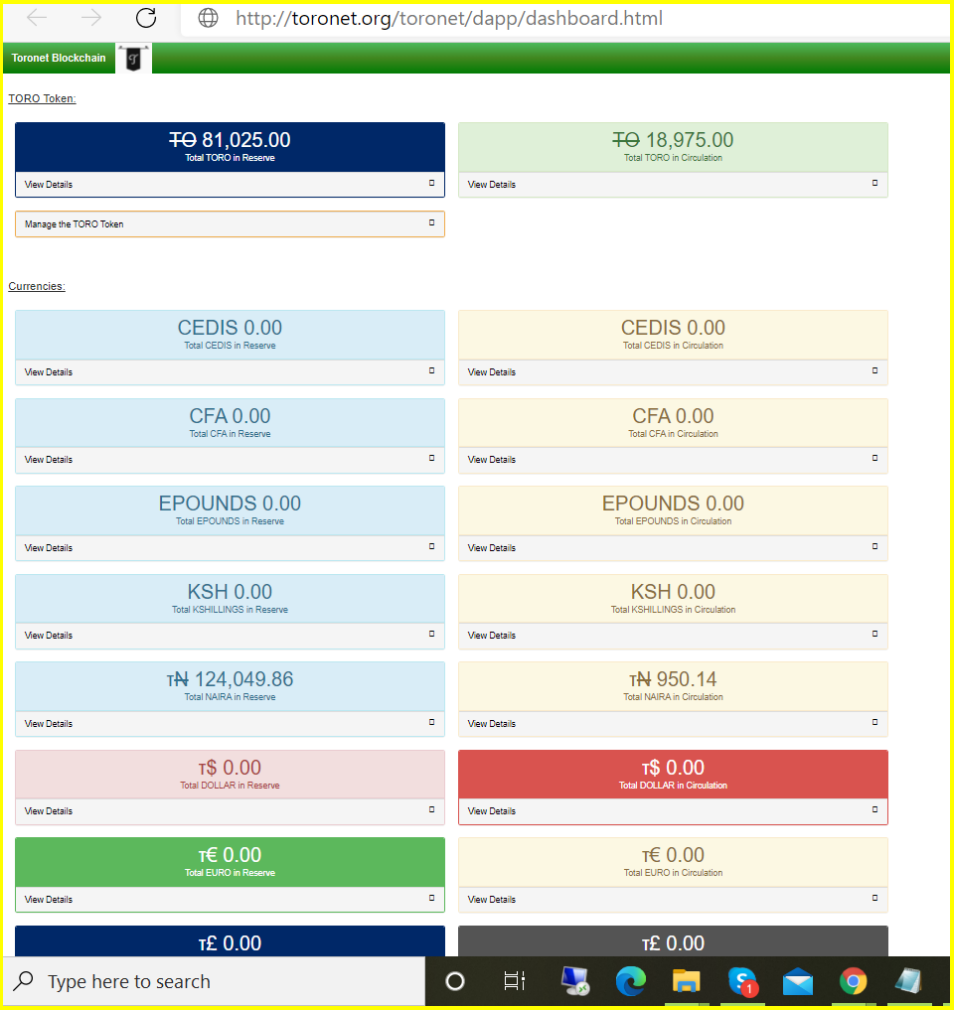

Figure 1. Multi-Asset Formulation of TǫrǫBlockchain

3.9 Support for Derivative Tokens

The TọrọNet blockchain includes derivative version of stable coins. These are tokens on the blockchain minted and backed by equivalent stable coin tokens coded programmatically on the blockchain to accomplish some contractual objectives. This allows developers to create their own tokens as derivatives of Toro.

There are several types of derived stable coins currently programmed in smart contracts on the blockchain, including:

1. Derived Stablecoins That Function Similar to a Escrow Payment

   An example of this is a contract for delivery of a physical asset. Such a contract may be funded by the buyer. The blockchain can then lock the funding in the contract and create a derivative equivalent in the same currency. The derivative stablecoin could then be paid to a delivery agent contingent on the ability of the delivery agent to "cash" the derivative or convert it back to the stablecoin on verification of delivery. The physical asset delivery contracts developed on the blockchain functions in this manner. Unlike a traditional escrow they do not require a third-party to initiate the release or conversion of the stablecoin as the conditions are coded directly in the contract and enforced by the blockchain.

2. Derived Stablecoins that Enforce Conditions of a Contract

   An example of this is a contract that issues a loan to purchase an auto vehicle. Such a contract may be funded by the loaner. The funding is retained in reserve while an equivalent stablecoin of the same value is generated. The derived stablecoin could be programmatically coded by the smart contract to only be convertible back to the underlying stablecoin by a user on the blockchain designated as an auto dealer. The derived stablecoin can then be provided to the borrower, who can only utilize the derived stablecoin to purchase an auto vehicle, by virtue of the instructions carried within the stablecoin asset's program. An example of this type of derived stablecoin is depicted in Figure 3.

3. Derived Stablecoins Programmed with Time Release

   Similar to the first two types of derived stablecoins, this version can only be converted to the underlying stablecoin maintained by the reserve under some condition. In this case, the condition is some time interval programmed by the contract and encoded within the derived token.

Other types of derived stablecoins may be constructed as new template contracts for real world finance and commerce are addressed on TọrọNetChain. Note that some of the derivative stable coins are expected to be transferrable or not depending on the terms of the contract as agreed upon by both parties. In all cases, the principle and goal is for peer-to-peer agreements enforced and managed by the blockchain such that third

party entities are not required to enable commerce or financial transactions between pertinent entities. This reduces costs, increases trusts, reduces risks, and potential default of contract terms.

3.10 Support for Non-Fungible Tokens

TǫrǫNet supports the ERC721 non-fungible token (NFT) standard. This standard was developed to define non-fungible tokens (NFTs) or more simply unique digital items. Similar to ERC20, adhering to this standard allows a uniform interpretation of unique asset tokens on devices and applications, regardless of the blockchain they are built on. The standard has since spawned growth in NFTs in 2021. Besides its use for tokenizing digital art, the application of this standard is currently leading growth of NFTs in the gaming industry and leading the pay-to-earn games phenomenon. Beyond securing digital art, this standard is also being used by nodes on the TǫrǫNet network to tokenize real-world items for buy now pay later BNL loans for items such as phones, using unique details such as their MEIs, auto-vehicles by their VIN and attributes.

3.11 Multi-Role Blockchain System

The TǫrǫNet blockchain by virtue of the type of smart contracts it fundamentally supports is designed to be a multi-role blockchain. This is distinct from virtually any other blockchain, but is necessary to make the blockchain useful in addressing the real financial and commercial needs of the communities it addresses. For instance, on the Bitcoin or Ethereum blockchain, all users of the blockchain have the same role and privileges on the blockchain.

On TǫrǫNet, all users start off with the same fundamental access. This includes an account, an ability to deposit funds, create stablecoin of equal value to fiat or crypto assets they deposit, transfer assets (make payments) to any other user on the network. However, to participate in some smart contract activities, several roles are created by the contracts, and users may apply to, or be assigned to those roles according to the terms of the contract. These roles provides the users access to features of different contracts to enable the terms of the contracts.

Currently, the blockchain includes the following default roles:

1. Operators	2. Loan Originators
3. Smart Phone Dealers	4. Auto Dealers
5. Mortgage Agents	6. Real Estate Appraisers
7. Agro-Dealers	8. Agricultural Produce Offtakers
9. Agricultural Produce Certifiers	10. Insurers
11. Farmers	12. Village Aggregators

A framework to create other roles is built into the network to accommodate other roles in future as more finance and commerce contracts are included.

References

1. Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). http://bitcoin.org/bitcoin.pdf, Accessed May 20, 2017.
2. Vitalik Buterin, Sep 1 2014, "Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform", https://github.com/ethereum/wiki/wiki/White-Paper, Accessed May 30, 2017.
3. Ken Alabs, July 2020, "A 2020 perspective on "Digital blockchain networks appear to be following Metcalfe's Law"", Electronic Commerce Research and Applications, Special 20 year issue, Volume 40 Issue C, March 2020, https://dl.acm.org/doi/abs/10.1016/j.elerap.2020.100939.
4. Ken Alabs, July 2017, "Digital blockchain networks appear to be following Metcalfe's Law", Electronic Commerce Research and Applications, Volume 24, July–August 2017, Pages 23–29 https://doi.org/10.1016/j.elerap.2017.06.003
5. The World Bank, March 4 2013, "Africa's Agriculture and Agribusiness Markets Set to Top US$ One Trillion in 2030", http://www.worldbank.org/en/news/feature/2013/03/04/africa-agribusiness-report. Accessed October 6, 2017.
6. Bitcoin Energy Consumption Index. Accessed May 20, 2017. http://digiconomist.net/bitcoin-energy-consumption
7. William Suberg, Jun 30 2017, "Ethereum Mining Needs More Energy Than Cyprus, Cambodia, Brunei" Cointelegraph, https://cointelegraph.com/news/ethereum-mining-needs-more-energy-than-cyprus-cambodia-brunei. Accessed September 12, 2017.
8. Li, Y. and Ang, K.H. and Chong, G.C.Y. (2006) Patents, software and hardware for PID control: an overview and analysis of the current art. IEEE Control Systems Magazine 26(1): pp. 42-54.
9. Evan Duffy & Daniel Diaz, June 14 2016," Dash: A Privacy-Centric Crypto-Currency", Dash WhitePaper, https://dashpay.atlassian.net/wiki/display/DOC/Whitepaper.
10. The Ideal Digital Currency http://www.trustnodes.com/2017/10/24/ideal-digital-currency
11. The Ideal Digital Currency Needs a Reserve Backed System http://www.trustnodes.com/2017/10/29/ideal-digital-currency-needs-reserve-backed-system
12. The Ideal Digital Currency Needs Scaling Solutions http://www.trustnodes.com/2017/11/05/ideal-digital-currency-needs-scaling-solutions
13. The Ideal Digital Currency Needs to be More Usable http://www.trustnodes.com/2017/11/12/ideal-digital-currency-needs-usability
14. The Ideal Digital Currency Needs to be Programmable http://www.trustnodes.com/2017/11/19/ideal-digital-currency-needs-programmable
15. The Ideal Digital Currency Needs Clear Regulations http://www.trustnodes.com/2017/11/26/ideal-digital-currency-needs-clear-regulations
16. The Ideal Digital Currency Needs to be a Force for Good https://www.trustnodes.com/2017/12/03/ideal-digital-currency-needs-net-force-good
17. Developing a Simple Feedback Page Requiring No Database Implementation (http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=7780&lngWId=4)
18. Ken Alabi, 2007, "Generation, Documentation and Presentation of Mathematical Equations and Symbolic Scientific Expressions Using Pure HTML and CSS", Proceedings of the Sixteenth International World Wide Web Conference (WWW2007), May 8-12, 2007, Banff, Alberta, CANADA http://www2007.org/posters/poster1015.pdf