FROM TRAD-FI TO DE-FI TO JASIRI

V1.0

BY

Celestino[e] Kariuki

kcelestinomaria127@gmail.com

jasiriprotocol.org

Date: February 22, 2022

Abstract

This paper is a first in a four-part series of papers that dig deep into the idea of the JASIRI protocol. We begin by going through the idea of a crypto-economic primitive, and how the protocol exemplifies that idea in how it works. We then go through the history of modern banking, and its current state and generally how JASIRI plugs in. Lastly, we will cover JASIRI's technical infrastructure, specifically its agencies, and the technical blockchain-native/cryptographic infrastructure powering the protocol as a whole.

Keywords

crypto-economics, smart contracts, blockchain-based finance

1.0 Crypto-economic primitives and JASIRI

Technically defined, the JASIRI protocol is a crypto-economic primitive that lowers the cost of micropayments and unlocks dead capital from real-world assets and commodities.

A crypto-economic primitive, solely defined, is a protocol-based incentive-driven system that is uniquely powered by a token and that wholesomely enables the coordination and allocation of capital to achieve a shared goal via the use of various programmed economic and cryptographic mechanisms.

There has already been many crypto-economic primitives preceding JASIRI in market, serving different goals to their consumers. Notable of them are:

1. Stable-coins: these are crypto-economic primitives that coordinate and allocate capital to maintain stability measured in a set ratio(e.g USDC – a cash and cash equivalent backed blockchain-based token maintaining a 1:1 ratio with the US Dollar).
2. The Ocean Protocol: this crypto-economic primitive uses *token-curated-registries* and *curved bonding* in its decentralized data exchange infrastructure. The *token-curated-registries* list participants in the network and the *curved bonding* is used to rate the relevance of the data provided.

Any true crypto-economic primitive functions as a self-sustaining system and has a resultant predictable coordination of a set of actors whether they be humans, organizations or machines. These actors consciously or unconsciously work and have their respective efforts result towards a specific outcome. The outcome is solving a specific problem in a highly reliable fashion. The best analogy would be the USDC Stable-coin as presented earlier.

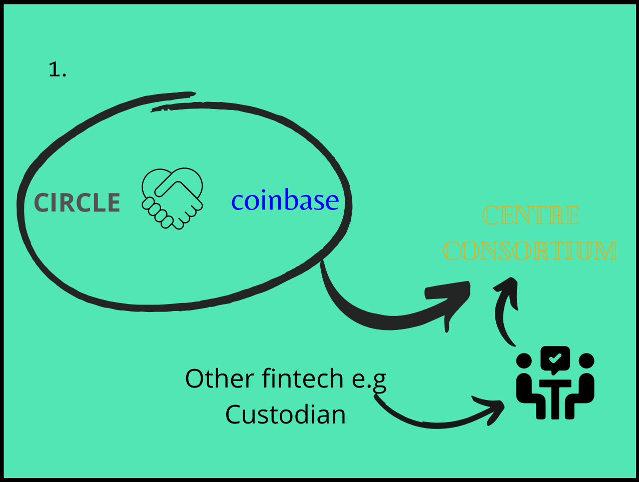


Figure 1: Circle and Coinbase partner to form the Centre Consortium

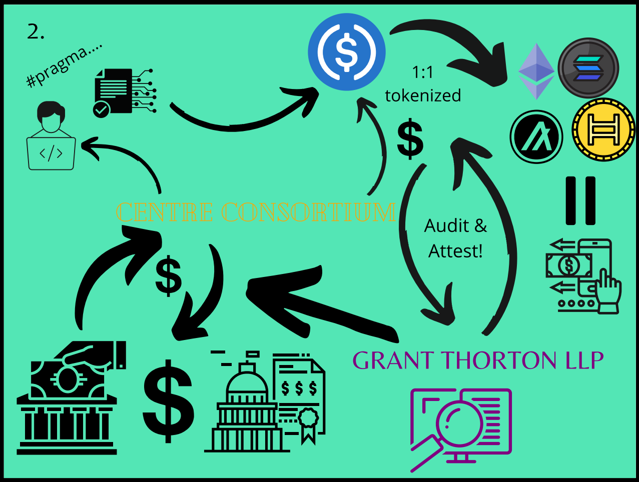


Figure 2: USDC, a perfect example of a crypto-economic primitive, is a fully reserved, fiat-backed smart-contractible stable token owned and managed by the Centre Consortium

1.1 High-level overview of JASIRI

Having defined JASIRI as a crypto-economic primitive, and sufficiently laid down how the concept works, it suffices now that we go through how JASIRI plays into that concept.

So, the JASIRI protocol crypto-economic primitive lowers the cost of micropayments and unlocks dead capital from real-world assets and commodities. The term ‘real-world’ can be misunderstood here, but it can be exchanged with the word ‘physical’ or ‘tangible’ for better understanding and context.

How does the JASIRI protocol unlock dead capital from these physical/tangible assets? Basically, in operation, an individual navigates to the JASIRI web dApp[1] or approaches any other JASIRI point of access to get some financing. We will call our random individual Bob.

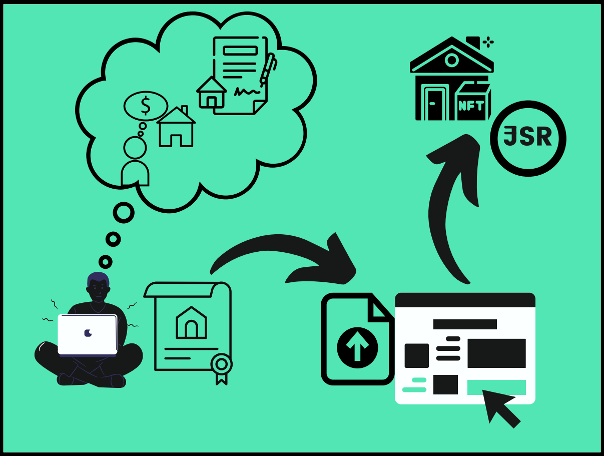


Figure 2: Bob visits the JASIRI Web dApp to tokenize his asset

After Bob tokenizes his physical asset at a 1:1 value[4] on the JASIRI protocol, he can, at any time he pleases, visit a JASIRI agent and get a hard cash or fiat value of his now live capital. Besides, he can also transfer his assets digital in the JASIRI ecosystem and swap his capital for other digital assets on various liquidity pools managed non-custodially on the blockchain.

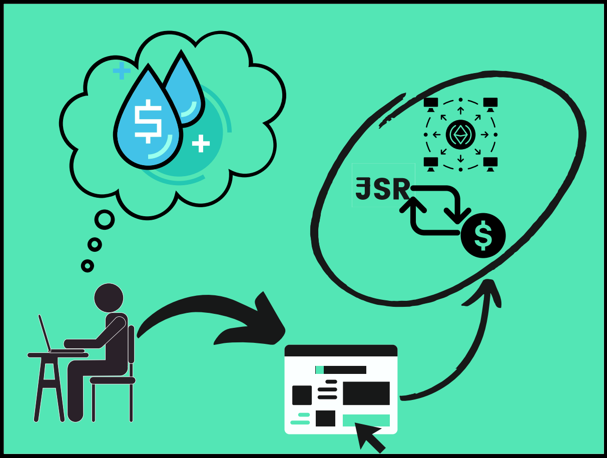


Figure 3: Bob can also easily source liquidity for his JSRs(JASIRIs) on the web dApp by swapping for other digital assets on LPs

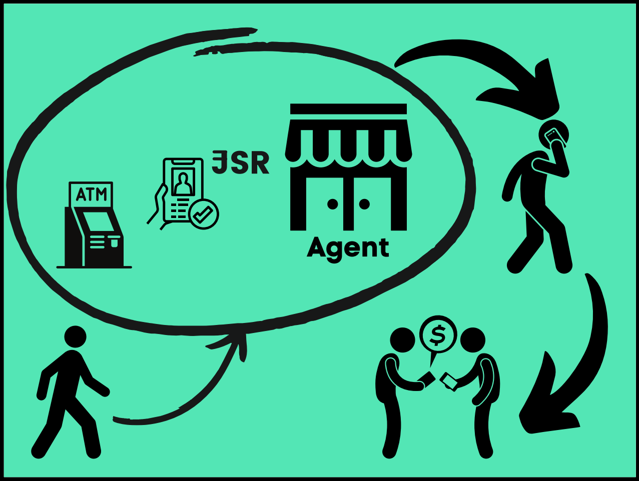


Figure 4: Bob can also visit a JSR(JASIRI) Agent or an ATM to get liquidity

Another question we need to answer, is how the JASIRI protocol lowers the cost of micropayments. This question pushes us into the analysis of its technical infrastructure.

The JASIRI protocol runs on the low-cost, layer-1 Algorand Blockchain[1]. Any transaction, such as the transfer of JASIRI assets(which of course is the most ubiquitous transaction type within the protocol), incurs a less than zero in value transaction fee. At the time of this writing, the transaction fees of the Algorand protocol is 0.001 ALGOs, which is almost less than 0.001 US Dollars. This is extremely low, and it means

[1] Web dApp means “Web decentralized Application”. Other naming conventions use Dapp, or DApp to mean the same. A Dapp/DApp/dApp is an application built on a blockchain, most of these applications are usually decentralized in an infrastructure setup, meaning you do not have the usual client-server app model like the traditional way of building applications, but rather you have a participant-based model.

that anyone, even someone living under the poverty line of $1, can make a transfer of JASIRIs from his account address to another.

The JASIRI protocol does not add any fee on top of the 0.001 network fee. Additionally, you are not required to purchase any crypto to start using JASIRI or to benefit from JASIRI's services.

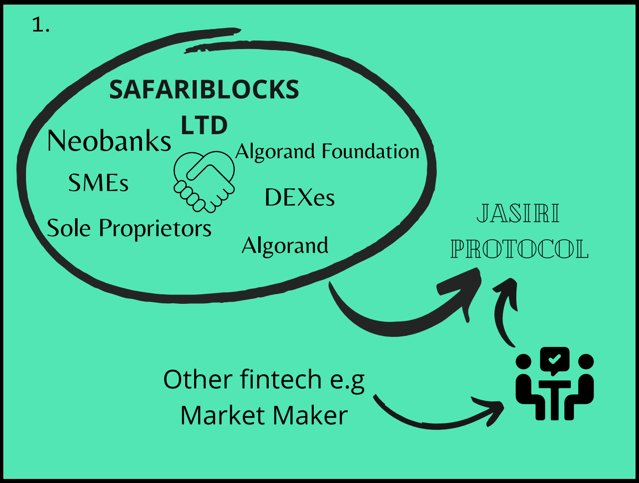


Figure 5: JASIRI Protocol as a crypto-economic primitive; Safariblocks Ltd & partners

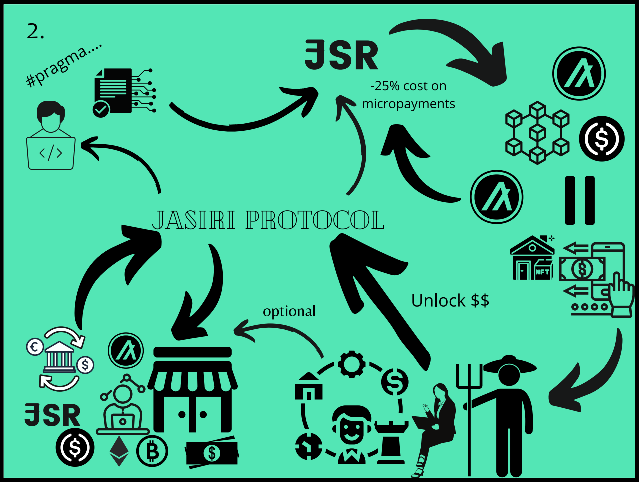


Figure 6: JASIRI Protocol as a crypto-economic primitive; JASIRI Protocol interplays with various organizations and human actors to achieve the goal of 'below zero' payments cost & transforming dead capital into live capital

The whole JASIRI way of moving capital of course differs with trad-fi's way.

In trad-fi, you typically make payments by using bank cheques or direct transfers, or what we simply call ACH-money. Of course, if you are East African, or coming from a region with deep mobile money penetration, you would use mobile money to receive or make payments.

The dominant mobile money infrastructure also uses agents for cash-in and cash-out processes, with a centralized mobile money operator or payment service authorizer securing the network. There is also a reliance on bank deposits to back the mobile money transactions/float through trust accounts. This intermediation and rent-seeking, typical of trad-fi technology, increases the cost of moving capital.

Figure 7: MPESA Mobile Money Service Agent Shop in Kenya, East Africa

1.2 Traditional financial systems, and JASIRI

Remember Bob? So, Bob visited JASIRI for financing. He probably needed to pay some bills, settle his kids school fees arrears, or just needed some working capital to run his hardware shop.

Bob, ideally, for any financing needs, should have visited a bank and get a loan or downloaded the latest fintech app on the App Store and apply for a loan. Loans are and have been for a long time the main avenue for financing throughout the history of mankind.

Historical consensus cites merchants around 2000 BC in Assyria as the inventors of the first prototype banks. During this time, farmers and traders transporting goods between cities needed some capital to drive their commerce and economic undertakings. They would therefore approach these savvy merchants who would ask them to only bring their grains. The merchants would then lend capital to the farmers and traders against these grains. This simple approach formed the mechanics of the lending process onwards, summarized as:

You need capital? Provide an asset to a financier. An asset, traditionally, is something that you own, and that has recurrent income. Once you provide this asset to the financier, you get lent the capital, with the financier assured to get ownership of your secured asset if you do not pay back the capital you borrowed.

For a long time throughout history, the money lending idea, hinged on providing an asset or property for custody and security in exchange for capital, was the dominant method of financing. Interest was of course charged on repayment, and in many cases lenders would charge high interest since there were no defined methods for risk-based pricing to evaluate the debtors ability to pay. The prevalent high-interest loans tainted the reputation of financiers, and it was only until Giovanni di Bicci de Medici, an Italian financier in the 1380s A.D[7], that the lending industry would get a shake up.

Since money lending was too risky, and the Catholic Church(the "regulator" of the day) condemned charging of interest as usury, Giovanni incorporated the idea of currency trading into the Medici family-run bank after realizing one could charge commissions on foreign currency exchange rates. With the Vatican as his main client, Giovanni made lots of profits from the currency exchange trade, eventually scaling up the Medici family-run bank, reinvestment the profits into the enterprise. This concurrently reduced reliance on the money lending practice.

Giovanni would also come up with the idea of bank deposits.

Depositors would be given *discrezione*[2] as compensation for risking money. This is similar to the modern savings rate or yield. With time, the Medici family-run bank would enjoy good reputation, and through Giovanni's son, Cosmo, banking the Medici-way would dominate the financial services industry in Italy at the time, taking institution of banking even closer to state power.

The Medici-way of banking has influenced modern banking in the 21st Century save for other edgy innovations.

In most financial systems, by a country or community basis, you have several retail and commercial banks that serve your average Joe, and then a central bank or reserve bank at the top of the hierarchy issuing currency and controlling supply. So as to easily reference this prevalent modern financial system throughout our paper, we will christen it – Trad-fi(Traditional Finance).

Loans are possible from a bank because of deposits. Deposits create loans. Bankers market to the public that if they put their hard-earned money into bank deposit accounts as savings, their money will earn recurrent passive yield in specific timeframes. Ideally, banks will take the deposits and go into the market to look for yield. The yield they hunt for should preferably account for the yield they will pay back to the saver for risking their money, plus some they can get for their enterprise as profit.

The best yield generators are usually brave entrepreneurs in the market building or starting profitable enterprises. A well-run enterprise is a money printer, albeit with more impact and value generation in society by virtue of creating what the common man wants. Bankers lend money to these enterprises on contracts, secure the enterprise as an asset, and get more back if everything goes as planned.

However, in today's age of the computer, banks can just record in a deposit from a saver, denote it as a liability, and electronically issue a loan "anchored" to that deposit as an asset. One may think that a deposit would be an asset to a bank, but some nuances would suggest the opposite. Idle cash loses value. Loans return more income to the bank, especially when contracted to a borrower under interest. Banks offer diverse offerings today, with additional, though limited, financing options for consumers provided they have an asset to collateralize.

Also, another way bankers use to get yield is to simply take the deposits or a portion of them to the capital markets industry if you live in a sophisticated market-driven economy. Capital markets "print money" through paper assets tied to real-world commodities or business structures but swayed in value by human speculation and consensus-driven fundamental value

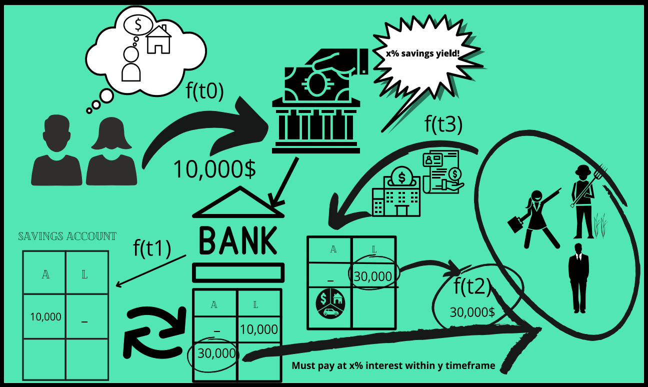
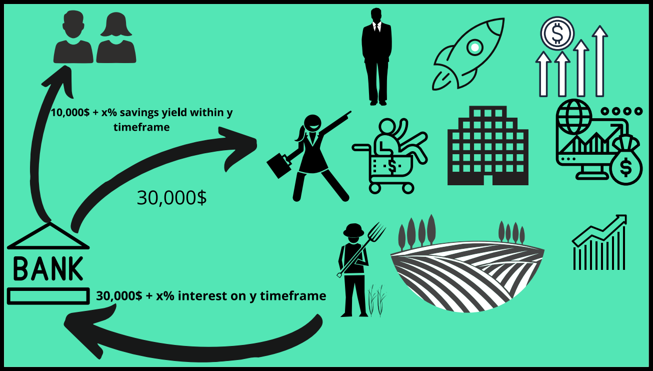


Figure 8: Vanilla Banking, from deposits to loans and back



10,000$ + x% savings yield within y timeframe
30,000$
BANK
30,000$ + x% interest on y timeframe

Figure 9: Vanilla Banking, loans and the economy

1.3 JASIRI's mechanics distilled

The JASIRI protocol introduces a fundamentally different process of financing from the lending process.

One recurring theme from the historical analysis of modern financing in section 1.2, is the idea that in order for you to get financing of any kind, you have to get an asset and then let the financier custody it in exchange for capital. JASIRI presents a paradigm shift from this.

At the core of the JASIRI protocol is a digital token. When Bob comes to JASIRI with his asset. This asset is digitized, and stamped on the protocol. JASIRI runs on the application layer of a layer-1 infrastructure blockchain. As the identity of this asset and that of Bob is stamped onto the protocol, subsequent value is made liquid. This value is captured from the asset's proof of buyer's receipt or deed. Value is unlocked directly rather than with Trad-Fi's lending approach which held that value in custody. We get deeper on this in the second paper[4] of this four-part series of whitepapers. Even so, the big picture of the whole mechanics is laid bare in the succeeding visual below.

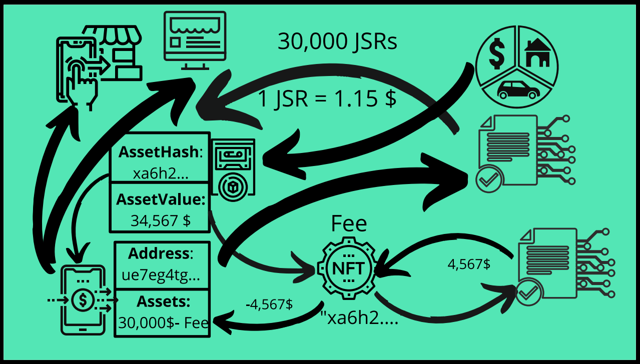


Figure 10: The JASIRI protocol's economic engine

Coincidentally, JASIRI's concept of having an asset being tokenized, and then having Bob, the owner of the asset, accrue debt-free capital right into his hands should remind us of something that happens frequently in trad-fi with central banks.

Strangely, this something similar is called quantitative easing. Let's get deeper into what quantitative easing is, and its parallels to JASIRI's mode of operation in the next section(section 1.4).

1.4 Chartalism, and JASIRI

We previously talked about the lending process, and how banks operate to avail this dominant form of financing in the modern economy. That's sadly not the end of the story.

Even as banks create loans from deposits, they have their systems and operations largely surveyed by central banks/reserves. Central banks collect data on deposits, loans and other banking metrics so that they can figure out the amount of money in circulation in an isolated economy. Banks also do put their reserves with central banks. This then gives them the insight to either print new money(by purchasing financial assets from banking/financing institutions, governments or other enterprises) to stimulate the economy or suck up money(by selling specialized financial instruments like repos[2] to banks, or reducing their purchases of financial assets[3]).

This process, known as quantitative easing(QE), is done by major modern central banks worldwide[2], accelerated as a formidable monetary policy mechanism at the backdrop of the 2008 global financial crisis.

Central banking as an idea first came about in 1668 A.D, with the establishment of the Riksbank in Sweden. The Riksbank, and many central banks launched thereafter(Bank of England etc.), mainly served the function of helping the government raise funds and also acting as a clearing house for macro-level, government-driven commerce.

It was Benjamin Strong[5], Governor of the Federal Reserve Bank of New York in the time duration 1914-1928 A.D, who would introduce the idea of open market operations[4], an important innovation in how central bank activities interact with the real economy, additionally reducing the direct role that was always played by central banks in financing the government.

This now meant you could have insurance companies, pension funds, banks, varied financial institutions and even daily cash-rich citizens looking for low-risk yield participating in bond-buying and many other activities provided for in open market operations.

JASIRI's form of financing is similar in its mechanics to the central banking QE and Open Market Ops process as you may notice, of course with the following nuances:

1) JASIRI does not purchase financial assets to inject liquidity into the economy, instead it "purchases" durable, day-to-day in use and explicitly owned tangible/physical assets.

2) While central banks directly print new money through QE[6][9], JASIRI only uses the internal coordination of the current state of an economy to put money back into people's pockets. Cash used to unlock capital in JASIRI is aggregated from the current money circulation regime in an economy through JASIRI's entrepreneur agents as well as on-chain AMMs(Automated Market Makers).

3) Central banks' policy of releasing money uses differing monetary policies, while many of these banks just use data to know when to print or suck up money as well as tighten or loosen interest rates, JASIRI uses a Proof of Asset™ policy(PoA™). A negative effect for the central bank's policy would be how to tame inflation as they inject new money. JASIRI's policy ensures money is only issued against tangible assets with very nuanced specifications.

[2] Repo, short for repurchase agreement, occurs when a central bank in an open market sells bonds to other entities, and agrees to repurchase those bonds later at a higher price with the bonds secured as collateral

[3] Central Banks reduce their purchases of financial assets in a process called "tapering". The result is mostly a decrease in the purchase of bonds(securities) initiated by the Central Bank.

[4] The goal of Open Market Operations was to keep inflation low and stabilize interest rates.

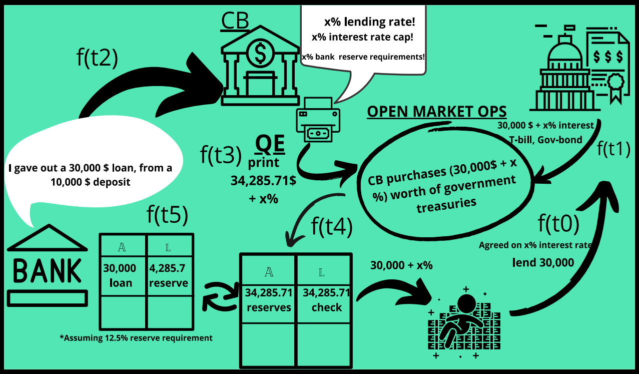


Figure 11: Money creation in the modern economy; f(t) refers to "a function of time".

1.5 JASIRI Agent Balance Sheet

So, after Alice on the JASIRI protocol has had her capital unlocked, they are of course denominated in JASIRI's native tokens.

Alice then goes to Bob, the agents so that she can get the unlocked capital transformed into something she can use on a daily basis to either do her trade, pay her son's school fees, or even simply buy some corn and vegetables to cook for her family the day's supper.

Bob's balance sheet dynamics is where we can interface with the real economy, and is especially affected by the money circulation regime.

We will try and picture the process in states and state transitions.

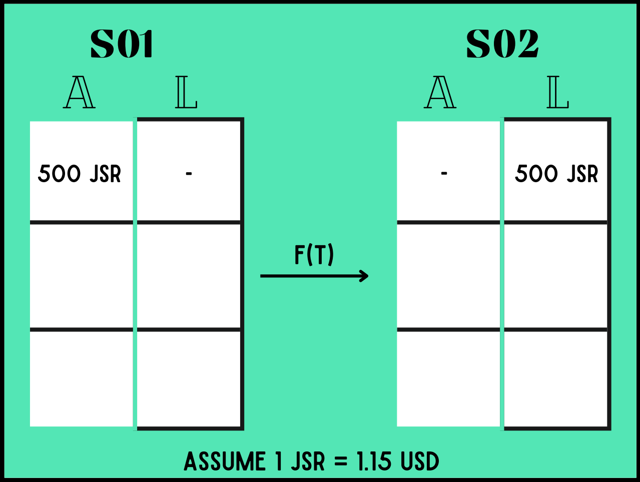


Figure 12: JASIRI Agent Balance Sheet; from State 01 to State 02

After Alice takes her 500 JSRs to Bob, Bob enters that as an asset, at State SO1, visualized above.

Capital is usually transferred using money, and as such, it loses value with time. The state transition function that moves Bob's balance sheet holding Alice's 500 JSR from State S01 to State S02 is mostly dependent on time as a variable.

In the previous section(1.4), we talked about the most common money circulation regime used today, and how it works. It is useful in understanding the transition from State SO2 to State SO3, and State SO4.

At any time, the amount of money in the economy is measured as(based on Figure 10):

$$Base\ Money(M_0) = 34{,}285.71\$,$$

$$here, M_0\ refers\ to\ the$$

$$money\ the\ central\ bank$$

$$has\ directly\ printed,$$

$$however, we\ can\ go\ further$$

$$and\ measure\ the\ amount\ of\ money$$

$$in$$

$$people's$$

$$wallets(checkable\ bank\ deposits$$
$$+ mobile\ money\ account\ balances).$$

$$This\ is\ more\ accurate, although\ we\ will$$

$$minus\ the\ reserve\ requirement\ amount,$$

$$leaving\ us$$

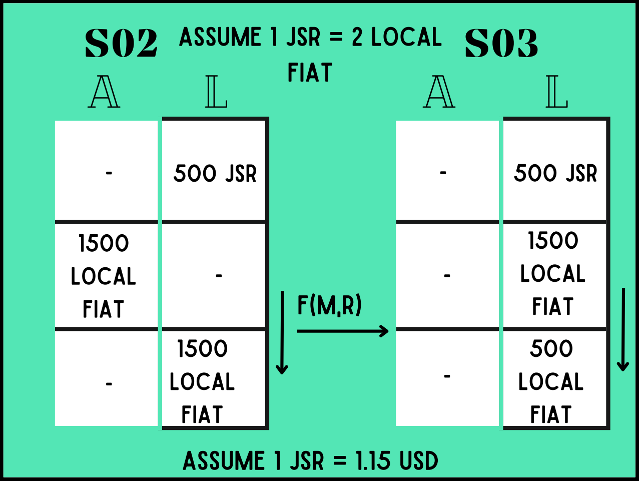
$$with: M_1 = 30{,}000\ \$\ from\ figure\ 11.$$

As a linear function, value of the base money will affect the lending rates, bond rates and the general amount of money in the economy.

With more money in the economy, we can expect that businesses will access loans at competitive rates.

Assuming our business agent got the 30,000$ loan. He reinvests that into growing his business, and makes more product sales. As sales grows, we expect Bob, our agent to make more revenues, and get visible profits, which will increase the availability of liquidity for the JASIRI protocol as well. This is all a cycle influenced by the central bank of the day and its monetary policy.

Since Bob, our agent is to give Alice her unlocked capital in her country's currency, he will use a % of his profits, investing into JASIRI in exchange for Alice's shiny JASIRI assets. Bob of course will have the imperative to do so since, as the money printing regime goes on, inflation and lower interest rates keep eating into the value of his cash holdings, so he needs to trade his cash(local fiat) for something that provides for competitive yield at reduced risk, which is what JASIRI provides.

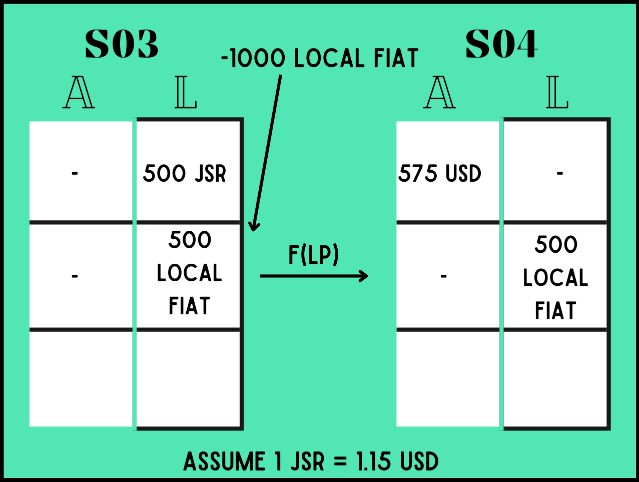


S02		S03	
A	L	A	L
-	500 JSR	-	500 JSR
1500 LOCAL FIAT	-	-	1500 LOCAL FIAT
-	1500 LOCAL FIAT	-	500 LOCAL FIAT

Figure 13: JASIRI Agent Balance Sheet; from State 02 to State 03

Above, 1500 Local Fiat represents the amount of cash Bob has committed, coming from his profits. It is of course a function of M(monetary circulation) + business revenues, denoted as f(M, R).

After giving Alice the fiat she needs, Bob can then proceed and explore the ecosystem for more yield, or simply just exchange for other digital assets as shown in the next visual. The state transition here is a function of the liquidity pools on the protocol.



S03		S04	
A	L	A	L
-	500 JSR	575 USD	-
-	500 LOCAL FIAT	-	500 LOCAL FIAT

Figure 14: JASIRI Agent Balance Sheet; from State 03 to State 04

1.6 JASIRI technical infrastructure

From an infrastructural perspective, interacting with JASIRI's assets is different from the trad-fi approach and more akin to de-fi with some nuances.

We earlier shared how trad-fi custodies capital, and how JASIRI unlocks capital and sets it free. To shed more light, we need to understand trad-fi's infrastructural features:

1. They can freeze your account or assets
2. Can censor or claw-back transactions
3. Perform rent-seeking that accumulates fees due to high levels of intermediation
4. No privacy
5. Opaque financial services' information, siloed databases and applications.
6. Requires a lot of trust from the customer that the infrastructure works as expected, and that he/she will get value from services offered. The customer has little control over their capital once they put it into trad-fi infrastructure.

Paralleling to de-fi[10], JASIRI offers the following infrastructural features:

1. Self-custody of your capital through a mobile wallet and other customized hardware solutions.

2. No one can censor or claw-back any transaction of your assets or commodities.

3. Protocol execution is automated by smart contracts and the underlying layer-1 blockchain infrastructure. The JASIRI team however centrally governs the standards for key processes like the quality-level of assets being tokenized, the community governance of the protocol, or the choice of business partnerships and agencies maintaining the health of the protocol, this borders JASIRI between pure De-Fi and centrally-governed but autonomous De-Fi.

4. While there is pseudonymity and privacy by default, identity solutions are still employed on JASIRI to prevent bad actors and support society in the fight against crimes like terrorist financing, and money laundering.

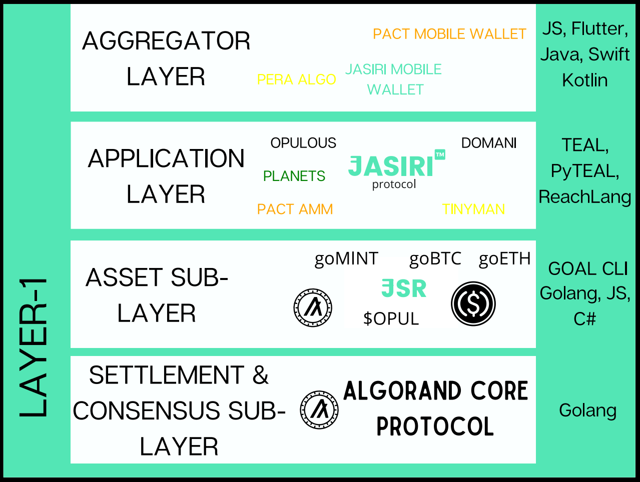


Figure 15: JASIRI's technical stack in the larger scope

Being built on the Algorand makes the JASIRI protocol possible, something that would be impossible if it were built on another chain.

It might seem strange or confusing that a JASIRI user must interact with ALGO tokens, aside from JASIRI's native JASIRI Tokens. While for the most part you do not need to buy any tokens to begin using JASIRI, you will still have to swap your JASIRI Tokens for some ALGOs so that you can fuel your transactions as you navigate the ecosystem for more services.

The main reasons why ALGOs cannot be removed from the equation is because of two things:

1. ALGOs secure the layer-1 infrastructure powering JASIRI, and also set the foundation for the decentralization of JASIRI.

2. The ALGO Token's low fees feature(<= 0.001 ALGOs) enables JASIRI to achieve Pareto efficiency in its distribution and allocation of capital.

In order to understand how ALGOs help secure and decentralize JASIRI, we need to get a glimpse of how ALGOs are used in achieving consensus on layer-1 Algorand using Pure Proof of Stake[1]. Here is how it works:

The Algorand network achieves consensus in two phases. In its first phase, a single ALGO is randomly selected from the network, from anyone's address holding ALGOs. So say, Alice has 1 ALGO, this 1 ALGO is selected and Alice is picked(in the background of course) to propose the next block to be produced.

In the second phase, 1000 ALGOs are also randomly selected from the network's holders(HODLERs), and they form a committee which will validate and approve the block that was proposed in the first phase by Alice's ALGO.

The selection of the committee members for the 1000 ALGO committee happens in a secure, randomized way leveraging on cryptographic primitives known as VRFs(Verifiable Random Functions), ensuring it is a fair process and that no one or not even a group of ALGO holders can gang up and attack the network. The assumption here is that in any society, the malicious players will never be "50% + 1" of the total players.

This secure process of block proposal, and propagation makes JASIRI secure, so we should all hold some

ALGOs, and participate in consensus to secure, and decentralize the network.

1.7 Agency Computation

JASIRI was built for the entrepreneur in mind, since day one.

To ensure honest, verifiable, and non-custodial computation between JASIRI's entrepreneur agents and its users, as well as in sync with the protocol, we need to implement a set of cryptographic primitives to power that computation securely.

One notable crypto primitive we will use will be the famous zk-SNARK primitive. This primitive should seamlessly interplay with the Agency infrastructure.

An entrepreneur agent is the prover in our system, and the verifier is a normal JASIRI user who needs some fiat liquidity.

For starters, drafting out the interactions would go like this:

$$i)\ Agent\ P\ will\ send\ w$$

$$to\ User\ V,$$

$$where\ w = fiat\ funds(secret\ witness)$$

$$ii) User\ V\ checks$$

$$if\ C(x, w) = 0,$$

$$where\ x = JASIRIs$$

$$to\ be\ withdrawn(a\ public\ statement),$$

and if true,

$$iii)\ User\ V\ sends\ x\ JASIRI\ assets\ to\ Agent\ P$$

However, some other things to consider that complexify the latter implementation are:

1) Due to privacy regulations, and policies, we do not want Agent P to reveal w to User V. This means we need it to be zero-knowledge, making w a secret. From a mathematical standpoint, we would have:

$$Agent\ P(S_p, x, w)$$

$$send\ proof\ \pi\ to$$

$$User\ V\ (S_v, x, \pi)$$

$$who\ then\ accepts\ or\ rejects\ the\ proof$$

$$For\ it\ to\ be\ zero - knowledge,$$

$$(S_v, x, \pi)\ should\ not$$

$$reveal\ anything\ about\ w\ .$$

$$Note\ that\ S_p\ \&\ S_v(used\ to$$

$$compute\ the\ desired\ outputs,$$

$$and\ represent\ setup\ procedures\ per\ circuit)$$

$$are\ derived$$

$$from\ pre - processing$$

$$the\ argument\ system,$$

$$such\ that$$

$$S(C) => public\ params(S_p(for\ Agent),$$

$$S_v(for\ User)).$$

There are various types of setup(denoted as S above) to summarize the arithmetic circuits[5] for User V. The best setup for our use case would be one that uses trusted randomness but has an updatable setup.

Such a setup would be achieved as follows:

$$S = (S_{init}, S_{pre}):\ where$$

[5] An arithmetic circuit is the basic computing model of cryptographic primitives and is used to implement systems in the blockchain space from a first principles standpoint.

$$S_{init} \text{ and } S_{pre} \text{ are}$$

$$\text{separate procedures.}$$

$$(i)\ S_{init}(\alpha) \to U, it$$

$$\text{generates secret randomness}$$

$$\text{that has to be destroyed once done.}$$

$$U = string,$$

$$while$$

$$(ii)\ S_{pre}(U, C) \to (S_p, S_v) \text{ which is}$$

$$\text{done deterministically and}$$

$$\text{is universally verifiable.}$$

The procedure (i), which represents the trusted setup procedure, is only needed to run once, and afterwards we can run procedure (ii) as many times as we want to generate as many arithmetic circuits. One thing to note is that with this setup, secret data in S(C)(The Standard setup for circuit C) is independent of C.

2) Also, integrating this proof system with trad-fi fiat systems risks making w long, and complex in computation. Our goal is to have a short, fast verification circuit in C(x w) .

A short proof is what should make our system succinct, and is mathematically guaranteed when,

$$\text{Agent } P(S_p, x, w) \text{ generates}$$

$$\text{proof } \pi$$

$$\text{such that } |\pi| = O(\log(|C|), \alpha),$$

$$\text{where } C \text{ here}$$

$$\text{represents the gates in the circuit,}$$

$$\text{also, at the same time,}$$

$$\text{User } V(S_v, x, \pi) \text{ must}$$

$$\text{accept or reject the proof}$$

$$\text{very fast}$$

$$at$$

$$time(V) = O(|x|, \log(|C|), \alpha).$$

$$\alpha = \text{security guarantees}$$

$$(e.g\ \text{crytographic salt})$$

3) While it is the User V specifically that needs the proof, we are forced to use an interactive argument of knowledge for starters. However, since we also want anyone in the JASIRI community of users to be able to verifier that the agent-user transaction took place, then we need to re-architect the proof system to be non-interactive.

1.8 JASIRI's principles vs mainstream crypto

JASIRI is built around a new model if you are thinking from the crypto world.

This new model is necessitated by the problems evident in the two major crypto innovation cycles, 1.0 and 2.0 until 2021.

I will simplify the crypto innovation cycle from 2009(with the creation of Bitcoin), to the start of Ethereum DeFi at the end of 2017[6] as crypto innovation wave 1.0. Crypto innovation 2.0 begins from 2017 to 2021.

We argue that there are deep flaws in the models of crypto innovation during these two cycles that have impeded widespread use and adoption of the protocols

[6] I timed the start of Ethereum DeFi with the launch of MakerDAO, but of course before this there were other attempts at DeFi products e.g EtherDelta etc.

and primitives developed during these cycles. We will go through each:

1. ***Users in crypto have always been required to buy crypto tokens using their money in order to participate.***

The repercussions of this approach have largely been damaging to the crypto concept and goals.

One, this concept has created lots of scams that have damaged credibility forcing the market to resist the whole crypto concept for long time now. Since Bitcoin's creation in 2008 to date(2022), crypto as a market has only been able to achieve a market cap of 1.9 Trillion US Dollars, which is dwarfing statistic as we can construe in the comparison table below:

Industry/ Company/ Product(2021-2022)	**Market Capitalization (In USD)**
NYSE Stock Exchange	27.69 T
NASDAQ Stock Exchange	24.56 T
Gold	12.23 T
Banks(Worldwide)	8.18 T
Shanghai Stock Exchange	8.15 T
Apple	2.80 T
Saudi Aramco	2.29 T
Microsoft	2.25 T
Crypto(Worldwide)	1.99 T
Google	1.81 T
Bitcoin	0.83 T
Visa	0.47 T
JP Morgan	0.388 T
Ethereum	0.385 T
USD Coin	0.051 T
Coinbase Exchange	0.037 T
Binance Exchange	0.018 T
Algorand	0.005 T
Uniswap DEX	0.004 T
Axie Infinity	0.00379 T

We chose to compare using market cap as a metric because Market Cap shows how much a product is worth, and also speaks the level of maturity of the product/industry or service.

By industry verticals, the crypto market is beaten by all incumbent competitors in market cap:

1. Exchanges(NYSE beats Coinbase by 784x, Shanghai Stock Exchange beats Binance by 453x, NASDAQ beats Uniswap DEX by 4,912x!!!)
2. Industry angle(Banking Services Globally beat Crypto Services by 4x)
3. Most valuable Big Tech(Apple), beats most valuable "Big Block" Ethereum by 7x.
4. Stores of Value & Commodities(Gold beats Bitcoin by 15x, Saudi Aramco(representing Oil/Energy) beats Bitcoin by 2.76x)
5. Mega Bank(JP Morgan beats USD Coin by 8x)
6. Transaction processing + payments/remittances powerhouse(Visa beats Algorand by 9.4x)
7. Gaming(Microsoft beats Axie Infinity by 594x)

All the above proves that the crypto concept and market is still very far from market adoption as shared earlier.

Secondly, this model of participation was skewed by the economic conditions of the Western world especially post-2008 and never accounted for the rest of the world even as crypto solutions are currently scaling globally. Even mining as a model of participation is not enough to make crypto solutions inclusive since a large demographic of the world population live in areas with low and costly energy output.

Close-to-zero interest rates in the West in the preceding years have made savings non-lucrative and forced Westerners to hunt for yield elsewhere as heralded by the growing retail investor movement(e,g. Robinhood app growing use, crowdfunding growth, wallstreetbets meme stock craze etc.). This caused high asset appreciation, most evident with the ridiculously high tech startup valuations today. This also meant that most Westerners viewed Bitcoin, and many other crypto as a potential avenue to store value(since bank savings do not work anymore) and get more yield for their capital. They viewed Bitcoin and crypto as investments, which even contradicts the initial goal of crypto developers which was to build a peer-to-peer payment system as evident in Satoshi's Bitcoin whitepaper[8]. However, whether to regard it as something good or bad, is not the point here, what to note is that the purchasing power of Westerners to a large extent will logically have an effect on the buying price of crypto products, buying out most crypto users in emerging markets, resulting in an unfair playing field.

Another repercussion is that, due to the high volatility of crypto(driven by fear and little understanding of crypto's use cases and fundamental valuation basis points), viewing it as an investment vehicle does not fit into play since lots of money have been lost as the concept is still very nascent, and many projects have little utility or use to anchor to.

For the developing world, requiring users to buy crypto in order to participate falls flat. Most of users in these regions live in markets with low fiat liquidity, punitive business environments, and largely government-driven economies that limit access to capital. That can be explained why at least play-to-earn crypto games, like Axie Infinity[3], have at least had success in emerging markets because they do not require buying of tokens to start.

JASIRI's primary mode of participation does not require anyone to buy crypto tokens or currencies to participate, ensuring there are no barriers to benefit from the financial services that the protocol offers.

2. *The deceiving, futuristic marketing of crypto products.*

Most crypto products are full of hype, promising so much in a very short time.

There is also a lot of FOMO from crypto users who are always constantly searching for the next coin that "will go to the moon".

With this perspective in check, JASIRI is clear of its proposition through its whitepapers, in order to set realistic expectations, and drive certainty based on tangible metrics, as well as explicitly share that the protocol is for use and not for short-term speculation.

3. *Highly volatile crypto market due to pervasive, and early-stage secondary trading markets*

Volatility in the crypto market is a distressing experience. For the most part, it can be attributed to the integration of advanced secondary trading markets into crypto markets, which abstracts decision on capital allocation to individuals and institutions who may not understand or have done due diligence on the value proposition of a crypto project, and just want to make quick profits and as such, will only seek price action.

This also adds a lot of unnecessary pressures to project creators, who can abandon a project's initial goals just to cash out.

As such, accessing JASIRI is only possible on primary market infrastructure natively found on a single decentralized exchange, with the rest channeled through its application. The amount of JASIRI Tokens issued on the primary market infrastructure are very limited and are meant for the early-stage asset price discovery of these tokens.

Acknowledgments

Special acknowledgements go to the following:

1. Allan Mang'eni, whose effort was instrumental in converting JASIRI's concept and ideas into actual usable products

2. Michael Burugu, who is the dominant brain behind JASIRI as an idea, particularly JASIRI's business processes, overall strategy, and the protocol's monetary policy.

3. Jay McCarthy, who dearly and selflessly assisted me, on an almost daily basis, to debug, and correctly write JASIRI's smart contracts largely programmed using the Reach Lang DSL.

4. Fabrice Benhamouda, who greatly influenced the security and usability decisions behind the JASIRI protocol, including the JASIRI Mobile Wallet, and who constantly assisted me during my builder's journey on Algorand from day one.

5. Autumn Moss Penaloza, & Johanna Moran, who welcomed me ever so dearly to the Algorand Community, and Algorand Ambassadors Community, and whose cordial, and level-headed support provided me conviction, strength, and the right resources to build JASIRI on Algorand.

6. The Algorand Foundation, who financed the development of the JASIRI protocol in its early stages, and the Algorand Foundation Team, most notably Kimberley Chang, Addie Wagenknecht, and Alan O'Connor, whose professional assistance, and stewardship steered JASIRI's progress and success during this critical early-stage period.

7. The Algorand Developer Community, specifically Jason Weathersby, and Barnji(Ben Guidarelli), who assisted with open consultation on the solution architecture of the protocol's code with respect to the Algorand transaction types, layer-1 primitives and the AVM(Algorand Virtual Machine).

References

[1] Algorand(2017). *A scalable, secure and decentralized digital currency and transactions platforms*: Algorand (github.com)

[2] Atlantic Council (2022). *Global QE Tracker* - Global QE Tracker - Atlantic Council

[3] Axie Infinity(2021). *The Official Axie Infinity Whitepaper*

[4] Kariuki, C. M. K.(2022) *Unlocking Dead Capital through the JASIRI protocol.* The JASIRI protocol whitepapers

[5] Liaquat Ahamed (2009) *Lords of Finance: The Bankers Who Broke the World*

[6] McLeay, M., Radia, A., Thomas, R (2014). Money Creation in the modern economy. *Quarterly Bulletin 2014 Q1*, Monetary Analysis Directorate – Bank of England: Threadneedle Street, London.

[7] Niall Ferguson(2008) - *The Ascent of Money. A Financial History of The World.*

[8] Satoshi Nakamoto(2008) – *Bitcoin: A Peer-to-Peer Electronic Cash System*

[9] *What is Quantitative Easing?* (2021). What is Quantitative Easing ? - Quantitative easing | Bank of England. Bank of England: Threadneedle Street, London.