

Ark Stack Development: An Interoperability Solution For Seamless Blockchain Ecosystem

Author, Balakrishnan Subramanian

A Data Science Foundation White Paper

January 2020

www.datascience.foundation

Copyright 2016 - 2017 Data Science Foundation

1. OVERVIEW

Ark - a decentralized mechanism invented to increase user assumption of blockchain technology. Ark plans to make a whole environment of connected affixes by giving simple to utilize devices to send our own blockchain. Being versatile and adaptable, it enables items to be procured by the across the board and make the use of the technology easier to use. It is available to any inpidual who needs to offer, or to develop their very own blockchain dependent on the Ark innovation stack by methods for having an open source code. For every 8 seconds a new block is created and it's resulting in phenomenal transactions.

2. INTRODUCTION

Blockchain operations are passing from demonstration around decentralized technologies to comprehensive result involving identity, data structures, crypto-economic designs, smart contracts and consensus mechanisms. In their convergence report Outlier Ventures stated that: "Most projects will fail, but the open-source nature of the ecosystem means learnings and code will be available to all". We can learn and build faster than ever.

1. Blockchain Technology: Concepts

Blockchain is a distributed and decentralized register, in which, set of blocks carrying a transactions are bind together by cryptographic array. Transactions start from a node is authenticated by engaging nodes and a set of execution are joined into a block by a "mining" node. The plenty of mining node enumerate power that resolves a cryptographic baffle can broadcast and generate a new block of authenticated transaction sets.

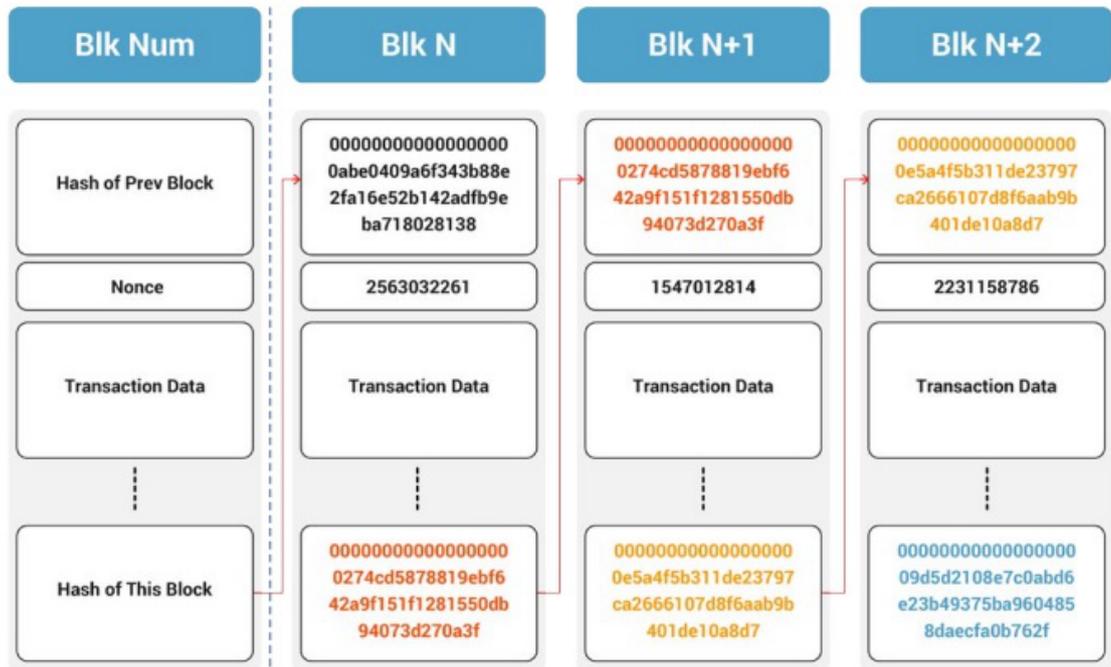


Figure 1: A Typical Blockchain Architecture (Source: SASKEN Whitepaper)

$$Block\ Hash = SHA2562(Hash\ of\ Prev.\ Block \ ||\ Nonce \ ||\ Tx\ Data\ Hash \ ||\ Time \ ||\ ver \ ||\ Target\ Value)$$

1. Peer-to-Peer Network

Blockchain employs peer-to-peer (P2P) network overspread on the Internet. It is shown in the Figure 2. Where every node interfaces with a set of adjoining nodes, each of which interfaces with their adjoining nodes and so on. At will any node can join and leave the network. Transactions and blocks are relay on the P2P network and each collecting node progress it to other adjoining nodes. Full nodes store a comprehensive copy of blockchain. Simple Payment Verification (SPV) nodes uphold payment using block headers, blocks are generated by mining nodes.

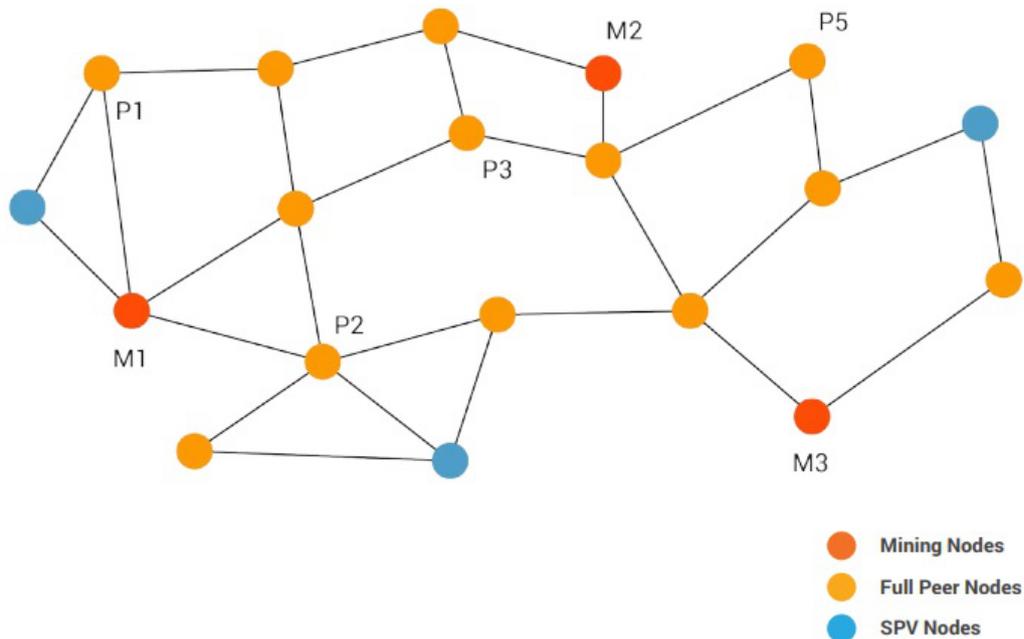


Figure 2: Blockchain Peer-to-Peer Network

2. Types of Blockchain

Blockchain can be classified depending upon how the nodes in the network join and the limitations placed on the roles

- permission-less or
- permissioned

1. **Permission-less blockchain:**

In this blockchain, by running the node software any node can join and leave at any point moment. The permission-less blockchain is also called as public blockchain. The peer nodes with private key verify the transactions sent by the signing transactions. The mere examples of this public permission-less blockchain are Ethereum blockchains and Bitcoin.

2. **Permissioned blockchains:**

Permissioned blockchains are at a corporation or association level (within an organization). Here, the contained information and nodes to be validated before connecting to the network. Here there are some limitations on the nodes that can justify and authorize the transactions. There are perse administration, but to be termed a blockchain rather than a distributed network, it must follow the decentralized idea with a dispense consent.

The perse blockchain open-source enactment are coming up with implementations such as Hyperledger and Ethereum, offering and aiding by industry magnate such as American Express, Cisco, Accenture, J.P. Morgan, IBM, Intel to name a few. The permissioned blockchain have well organized concurrence algorithms such as Practical Byzantine (PBFT), Proof-of-Authority (PoA) and Proof-of-Elapsed-Time (PoET).

3. Smart Contracts

Smart contracts blockchain are computer cryptogram which performs contract requirement linking functions positioned on the blockchain. It implements and executes the contract completely or moderately as per the cipher contract, electronically based on the occurrence. For example, product might have a smart contract for stock procure which must be carried out on time. But there can be constrains on payment with penalty deducted, no payment, full payment etc. This can be stationed and coded on the blockchain. IoT devices can stimulate this events and dispatch to the blockchain. Imagine if there was a hamper in the shipment entering at the buyer's location, with the entering affair and automated time sent by IoT device to the blockchain, the account makes a payment self-regulating with penance debit to the merchant.

4. What is Ark

ARK delivers revolutionary blockchain technologies to the startups, users and developers. To make ARK scalable, highly flexible and adaptable, we train to design a whole ecosystem of connected chains and an effective spiderweb of countless scenarios. ARK is a closed platform drafted for massive endorsement and will transport the favor of developers demand and consumers desire.

5. How Does Ark Work?

The squad is establishing various remarkable characteristics into the ecosystem - all with the underlying, integrated objective of creating a blockchain more reachable to the world:

- SmartBridges
- Alternative Programming Languages
- Push Button Deployable Blockchains
- SmartBridges - Disparate blockchains cooperatively through the Ark core platform. Primarily, Ark turns the mediator linking contrasting chains enabling them to interface with one another and activate events across chains - something that isn't happening viable.
- Enabling SmartBridges on a chain is an effortless way as placing a fragment of code.
 - While ARK was developed on Node.JS/Javascript, the company wants developers to be comfortable using their programming language of choice. As a outcome, ARK has united the following languages: Ruby, GraphQL, Python, Elixir, Nucleid, C, C++, Rust, Java, PHP/Laravel, Typescript, Symfony, Kotlin, Go, .Net, Lua, RPC and Swift iOS.
- Interchanging Coinbase and Shapeshift may additionally an advantage for SmartBridges. While still demanding their normal transaction percentage, these

platforms can utilize encoded listeners to react as a channel for SmartBridge transactions.

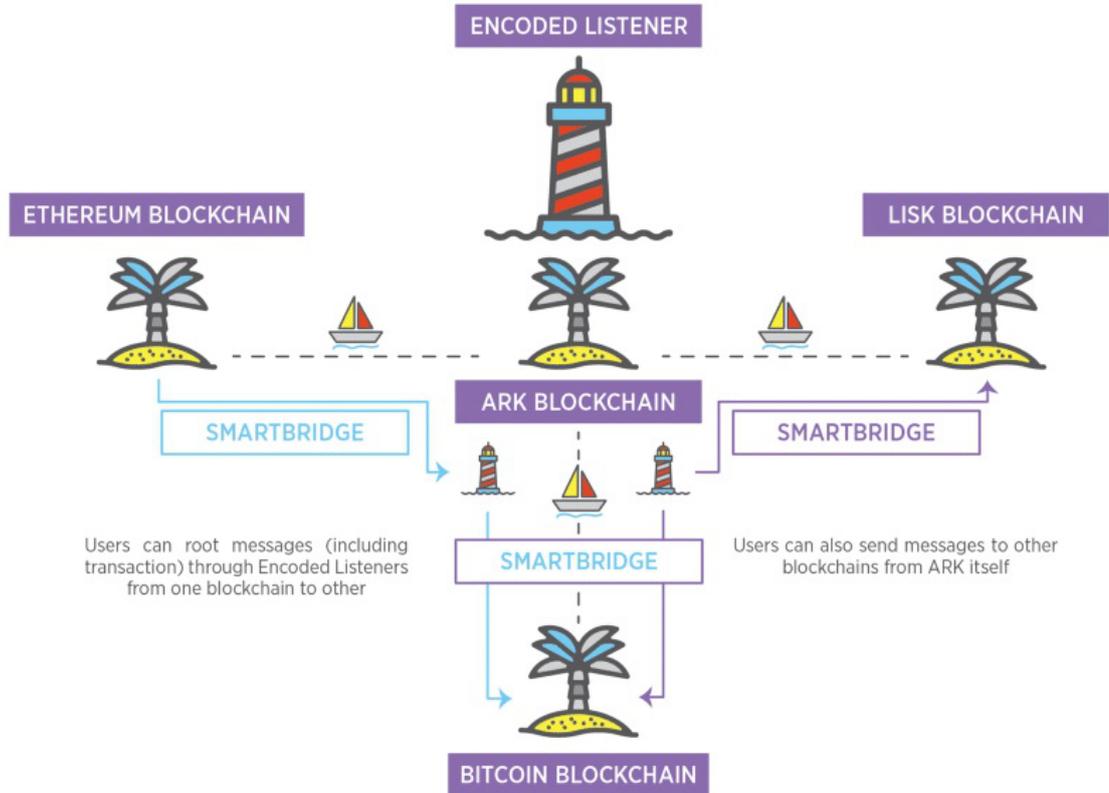


Figure 3: Ark SmartBridges and Encoded Listeners

3. HOW ARK ADD VALUE TO THE BLOCKCHAIN TECHNOLOGY?

ARK's bit of leeway declaration rest inside that focal stage and the estimation of the arrangement we are incorporating with the biological system. Administrations, for example, the capacity of interfacing with various blockchains through our SmartBridge innovation. It is appeared in the Figure 4. We have effectively associated with Ethereum, Bitcoin, and Litecoin blockchains with additional being developed. SmartBridge permits ARK to move information starting with one blockchain then onto the next with the utilization of unique Encoded Listener Nodes that can decipher and process information to and fro between various chains. With the reconciliation of one of our next achievements, ArkVM, all ARK blockchains will be equipped for using savvy contracts too and we are simultaneously chipping away at an IPFS based blockchain storage solution.



Figure 4: ARK SmartBridge concept Sending BTC to an ARK Address

4. DEVELOPING OPEN-SOURCE SOLUTIONS BASED ON ARK ECOSYSTEM

ARK understood that from the beginning and characterized the building blocks of the environment, together with the network. The result is one of the tying areas in the crypto space. With in excess of 12,000 day by day dynamic clients you get every one of the advantages of the OSS model conveyed to you. Cost decrease, quality improvement and speedier time to showcase are only a portion of the increases you get by joining our locale.

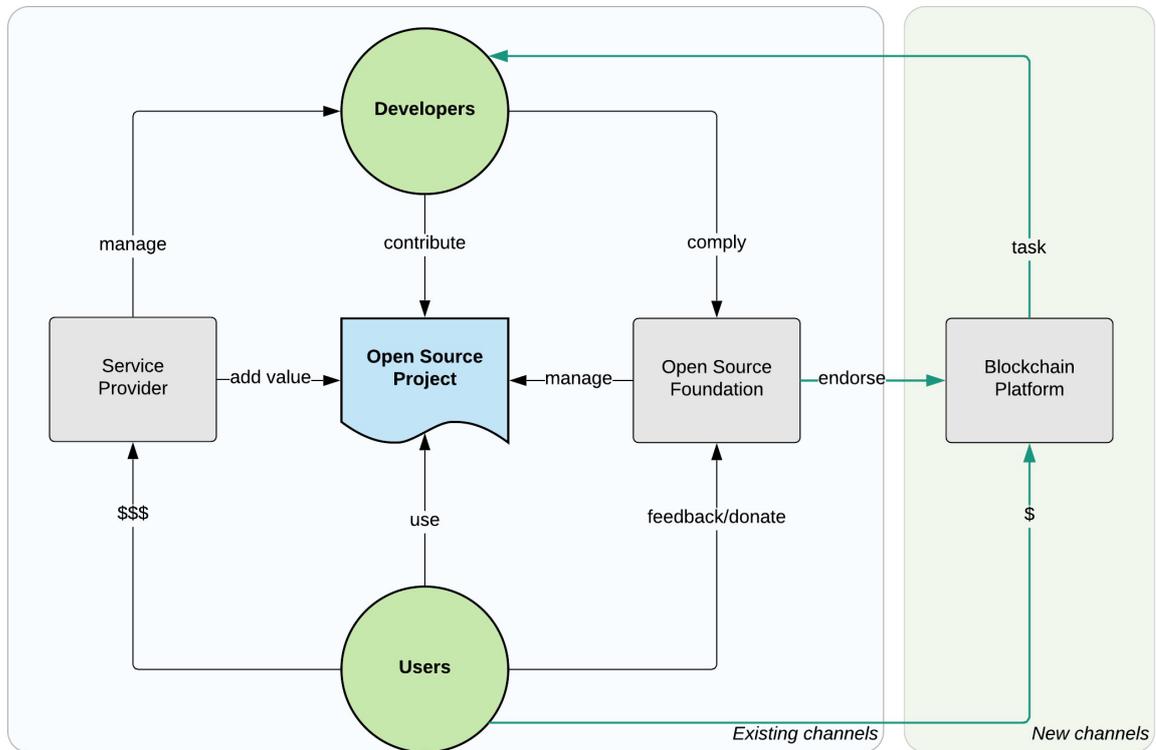


Figure 5: The usage of blockchain in the open source ecosystem

5. BIGGEST BLOCKCHAIN CHALLENGES - INTEROPERABILITY

Interoperability simply means inter- and cross-blockchain communication. Interoperability should be addressed at different levels.

ARK is at its core defined to address the challenge of interoperability with its SmartBridge field. To solve this problem, we are using the following technology:

- ARK Deployer
- ARK ACES (Aces Contract Execution Services)

It is an ideal case of an answer tending to interoperability issues between various blockchains and is created as a network venture for anybody to participate and help improve and include new highlights or report issues confronted when utilizing ACES.

1. ARK Deployer

To design your personalized ARK based blockchains ARK Deployer is a superficial deployment manuscript. Developers can design their inpidual blockchain in a medium of

minutes, by utilizing the ARK Deployer. ARK Deployer is the initial phase in establishing a more robust ecosystem that will be customizable, user friendly, and will attribute the same excellence of user interaction that you anticipate from an ARK conception.

ARK Deployer employs, incorporates, and configure the following:

- On a single server/computer, ARK Deploys Core Testnet in auto-casting mode, with casting generation delegates (sets custom parameters and clones the ARK Core, generate an outset with auto-casting delegates).
Note: to auto-forgo on Mainnet and Devnet, the delegates.json file needs copying as per the instructions at the end of the install.
- Configures the ARK Deploys Explorer and talks with the established ARK Core (integrates, clones, installs and configures ARK Explorer with the ARK Core).
- To start traversing it configures ARK API for the developer, hacking and expanding outcomes deploys on ARK Core technology.

The ARK Deployer v2 provides the base for our upcoming graphical interface product (GUI version) that will allow for blockchain creation,

2. ARK Contract Execution Services (ACES)

ARK Contract Execution Services is the principal working use-case of ARK's SmartBridge innovation. ACES starting discharge makes for a different universe first for ARK, by connecting two separate blockchains together and accomplishing genuine interoperability between environments.

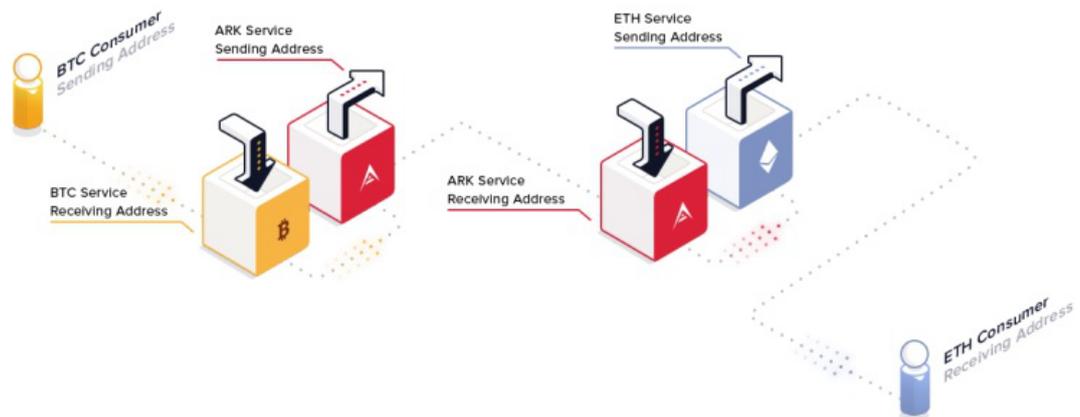


Figure 6: ARK ACES concept

ACES additionally permit clients and engineers to compose and execute brilliant agreements on Ethereum (ETH) by means of ARK. Utilizing ACES to compose Smart Contracts on Ethereum is an achievement in blockchain innovation. It shows the genuine intensity of

ARK's SmartBridge innovation. This administration requires a further developed comprehension of Ethereum Contracts and the Ethereum Solidity language. It is given in the figure 6.

6. ARK CORE V2 - THE NEXT FRONTIER

ARK-center v2 is totally configurable, which means you can modify the blockchain mechanics to your favored arrangement. Clients can modify block times, number of delegates, block size, customize fees and set block rewards. This design is a living arrangement, which means it tends to be balanced when your arkchain is running, all you have to give is the square stature parameter - from where the new setup will be legitimate and being used.

The new architecture (see Figure 7) has been entirely changed to separate delegate activity threads, conduct pool management and API interface on different actions. Transactions will need to move whole Simple Payment Verification (SPV) on an individual process or before striking the server mempool, sandboxing the whole action of the nodes against shells.

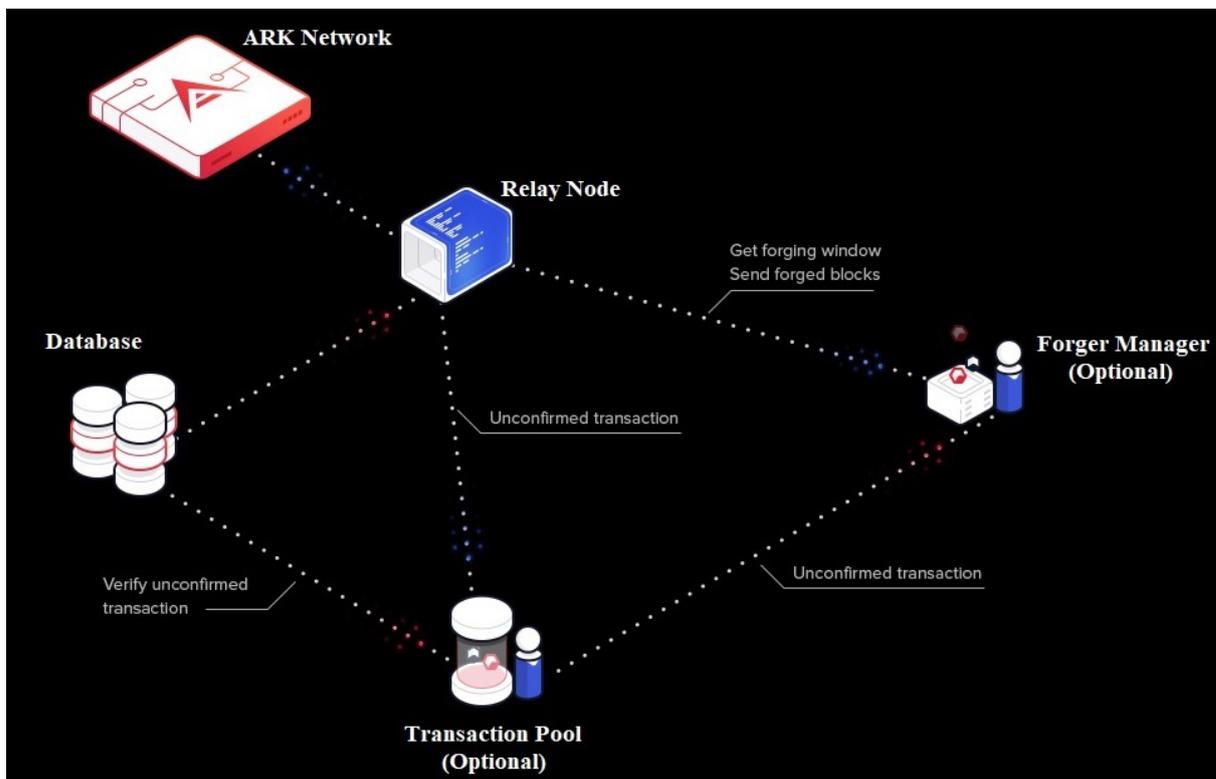


Figure 7: Initial Architecture of the ARK CORE v2 Prototype

It merely takes about 1 minute for ARK core to accomplish mandatory initialization, after the successful download of database. Checks and SPV rebuilds are shown in the figure 8.

```

fixcrypt@fxs-MacBook-Pro ~/g/a/ark-core> npm run start:mainnet
> ark-core@1.0.0 start:mainnet /Users/fixcrypt/git/arkio/ark-core
> NODE_PATH=. node app/start-relay-node.js -c config/mainnet

[2018-02-24 05:04:42] [INFO] : Initialising Dependencies...
[2018-02-24 05:04:42] [INFO] : Initialising Queue Manager...
[2018-02-24 05:04:42] [INFO] : Initialising Webhook Manager...
[2018-02-24 05:04:42] [INFO] : Initialising Database Interface...
[2018-02-24 05:04:42] [ERROR] : Unhandled Rejection at: [object Promise] reason: Error: connect ECONNREFUSED 127.0.0.1:6379
[2018-02-24 05:04:43] [INFO] : Initialising P2P Interface...
[2018-02-24 05:04:43] [INFO] : Oh hapi day! P2P API is listening on http://fxs-MacBook-Pro.local:4001
[2018-02-24 05:04:45] [INFO] : Looking for network peers
Peers Discovery [=====] 100% ✓
[2018-02-24 05:04:50] [INFO] : Found 11/46 responsive peers on the network
[2018-02-24 05:04:52] [INFO] : Looking for network peers
Peers Discovery [=====] 100% ✓
[2018-02-24 05:04:57] [INFO] : Found 149/184 responsive peers on the network
[2018-02-24 05:04:57] [INFO] : Initialising Blockchain Manager...
[2018-02-24 05:04:57] [DEBUG] : event 'START': "uninitialised" -> "init" -> actions: ["init"]
[2018-02-24 05:04:57] [INFO] : Fast rebuild: false
[2018-02-24 05:04:57] [INFO] : Last block in database: 3622877
[2018-02-24 05:05:03] [WARN] : lost cold wallet: 14owCmVdn8SaAFZcLbZfCVu5jvc4q7Tm1 699990000000
[2018-02-24 05:05:03] [WARN] : lost cold wallet: 151CWqrw1mWnD0GekCznF6Z5jKvivrWApp 10
[2018-02-24 05:05:03] [WARN] : lost cold wallet: 1M15BKbXQzhEvdCQXdtRthkPW7ryS1p8g 490000000
[2018-02-24 05:05:04] [WARN] : lost cold wallet: TobY8GSeuAkpDQFM9rdz6QadmMfsw3wnoS 3419817844
[2018-02-24 05:06:15] [WARN] : Negative balance should never happen except from premining address: AewxfH0obSc49a4radHp74JZCgPBLRe4xA--125000000.00000004
SPV Building [=====] 100% ✓
[2018-02-24 05:06:19] [INFO] : SPV rebuild finished, wallets in memory: 81485
[2018-02-24 05:06:19] [INFO] : Number of registered delegates: 656

```

Figure 8: Initialization of ARK Core

7. NEW PLUGIN SYSTEM - ARK Core v2.3

One of the major changes in ARK Core v2.3 is the introduction of the Generic Transaction Interface (GTI). The first iteration of this interface will make the ARK Core even more versatile. GTI is a prerequisite for upcoming developments including the much anticipated new transaction types—multisignatures, timelocks, multipayments and more.

There are 3 major components of this newest release. Each one makes Core stronger, provides additional functionality and streamlines our development process moving forward. With the ability to create new, standardized transaction types, v2.3 makes ARK more extensible and easier to modify for our bridgechain community.

- AIP 29: Generic Transaction Interface
- Increased Vendorfield Size (64 to 255 Bytes)
- Full SHA256 Block ID's

8. ARK TESTSUITE BASED ON JEST TECHNOLOGY STACK

Few software developers are up to date of how hardened is to get load test analysis over dissimilar testing stages that must take many stakeholders into register. By adding blockchain mechanism, and figure out how to block propagation, test distributed systems, fork management, client API, transaction pool handling and security mechanics get dicey.

Considering these obstacles in mind, it was a foremost to select the accurate tool which is workable and robust enough. Deciding that the Jest Framework foremost match ARK as the base testing framework, especially compute the market options. In Facebook Jest was used to test all the JavaScript code counting React applications. Jest framework is also used by Oculus, Pinterest, Instagram, Twitter and Airbnb.

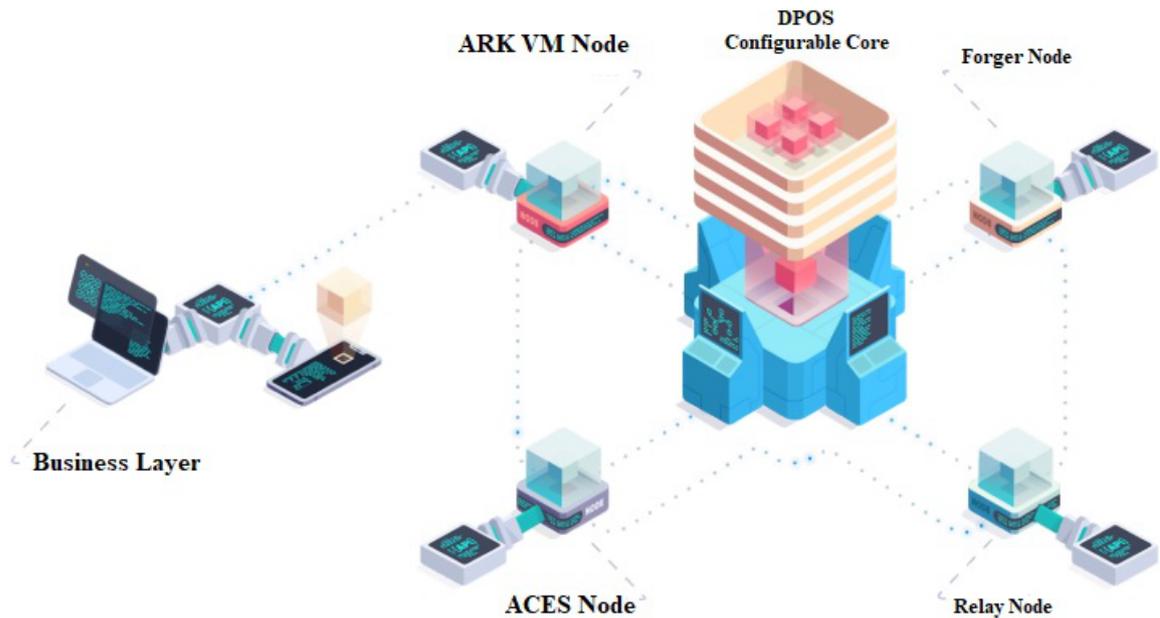


Figure 9: ARK Technology stack Parts

9. THE ROADMAP

Throughout worldwide the Blockchain technology caused a new rejuvenation of inspiration. Among thousands of blockchain ventures are in the space, working products and satisfied assurance are emerging to take shape and the potential for this technology is tremendous.

A fortunate ARK Ecosystem means that hundreds, if not thousands, of enterprises, organizations, communities and businesses are using ARK technology to establish blockchains practice modified to their needs. Further blockchain plans with manifestation on a restrictive mainnet begun to shatter off and form their own ARK-based network, labeling their scalability distress and extending bigger standards of variability using ARK Logic.

About the Data Science Foundation

The Data Science Foundation is a professional body representing the interests of the Data Science Industry. Its membership consists of suppliers who offer a range of big data analytical and technical services and companies and individuals with an interest in the commercial advantages that can be gained from big data. The organisation aims to raise the profile of this developing industry, to educate people about the benefits of knowledge based decision making and to encourage firms to start using big data techniques.

Contact Data Science Foundation

Email: admin@datascience.foundation
Telephone: 0161 926 3641
Atlantic Business Centre
Atlantic Street
Altrincham
WA14 5NQ
web: www.datascience.foundation

Data Science Foundation

Data Science Foundation, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ
Tel: 0161 926 3641 Email: admin@datascience.foundation Web: www.datascience.foundation
Registered in England and Wales 4th June 2015, Registered Number 9624670