ARK.io

Point. Click. Blockchain.

ARK Ecosystem Whitepaper
Version 2.0.0 | April 1, 2019

Abstract: *ARK empowers everyone, regardless of their aim or technical background, to quickly and easily leverage blockchain technology. Our whitepaper will identify the well known problems within the blockchain industry and illustrate how ARK technology solves them. In this current landscape of hype and empty promises, ARK acts as a beacon for individuals, enterprises, and communities who wish to make a real difference and apply blockchain technology to reach their individual goals as well as improve society. ARK offers a technology stack, unique in its simplicity, to create and deploy standalone blockchains for any use case. These newly created blockchains will have the ability to interoperate through ARK SmartBridge Technology. ARK is also turning Smart Contracts on their head with what is called ARK Logic, a collection of tools including custom transaction types, templates, and plugins. This brings decentralized computing and workflows into a more secure, adaptable, and scalable environment. Most importantly, the ARK Ecosystem fosters a growing international community of developers, node operators, blockchains, businesses, and enthusiasts, breathing life into this breakthrough technology.*

*The whitepaper is fluid and ARK is open to community feedback. For a deeper technical dive into ARK technology, visit **docs.ark.io**.*

Table of Contents

▲ 1 Introduction

1.1 State of the Industry

We are ten years into the decentralization revolution, since the publication of Satoshi Nakamoto's paper and the introduction of the first decentralized solution to solve the problem of double spending in digital networks [1]. Currently, we are moving through the phase of disillusionment where interest wanes as experiments and implementations fail to deliver. Producers of the technology either succeed or give up. Blockchain projects are now moving from experimentation around decentralized technologies to complete solutions including consensus mechanisms, identity, data structures, crypto-economic designs and Smart Contracts. In order to deliver truly world-changing results with blockchain technology, it must be easy to access for the majority of developers, users, governments, and businesses alike [2].

1.2 Eliminating the Barriers to Entry

ARK is looking to eliminate the barriers to entry in the blockchain space that are caused by the immense complexity of the technology. We are making that a reality by steering our efforts toward meeting the needs of enterprises, start-ups, and developers as our prime customer base. ARK aims to become a global backbone of decentralized application-centric blockchains, which we call *bridgechains*, which will allow them to either work with each other or stay isolated in their own environment. Chains that need to exchange data or expand their business models and use cases will find it very beneficial to utilize our global highway as a decentralized communication layer, thus unlocking the full power of Web 3.0.

1.3 ARK as the Perfect Starting Point

The ARK Ecosystem is an ideal environment for future blockchain developers. ARK will allow them to customize a sovereign blockchain for their needs, complete with the required feature sets at their fingertips. ARK's value proposition lies within the Core platform and the utility of various services, such as connecting to different blockchains, introducing custom business logic, developing new tailored transaction types, accessing a global support system through the community, and much more. ARK has six core values that act as the compass by which ARK navigates the rough seas of blockchain, but first, it's important to explore the current issues and challenges with blockchain technology.

▲ 2 Blockchain Trilemma

2.1 Blockchains Have Problems

Looking at the first wave of blockchain platforms, a well-known set of issues and challenges have arisen [3]. These issues include:

Scalability, handling large volumes of transactions at high speed
Interoperability, independent chains exchanging value and instructions
Sustainability, creating self-sufficient and self-governing environments

All of the above challenges are tightly coupled with the *Blockchain Trilemma*, identified by the balancing act blockchains face between *Scalability*, *Security*, and *Decentralization*. We took this trilemma very seriously when we set out to develop the ARK technology stack. All three properties are linked, meaning if we want to increase one property, it will most likely force tradeoffs with others. For example, the Bitcoin network optimizes for security and decentralization at the expense of scalability. Bitcoin scalability issues became apparent with the high transaction fees the network saw in late 2017 [55]. One approach Bitcoin is taking to resolve the issue is the advent of layer two solutions like the Lightning Network [4].

2.2 ARK's Approach to the Blockchain Trilemma

We believe ARK to be a true balance of scalability, security, and decentralization. ARK is addressing scalability through a multi-chain approach and ARK SmartBridge Technology. Defined business processes with high complexity can be run and supported on a bridgechain, and only its results would be transferred back to the main chain. Security takes shape through a modified version of Delegated Proof-of-Stake, where token holders determine which nodes are deemed worthy to secure each network, and nodes with the power to create or *forge* new blocks are in constant flux. Decentralization is left up to the needs of the system architects, as ARK's flexible technology can expand to include thousands of nodes, or contract to a few high-powered nodes capable of breakneck performance. Developers using ARK technology have the power to optimize each network as needed. ARK's six core values come together to allow ARK to tackle the Blockchain Trilemma.

⬛ 3 ARK Core Values

3.1 Simplicity

ARK believes first and foremost that in order to facilitate widespread use of blockchain technology, it must be made simple both for users and developers. ARK takes this statement even further by integrating it into the fabric of its tools, projects, and products. ARK is casting a very wide net to capture as many people as possible, and they will be able to deploy blockchain technology to solve their problems and realize their visions. Just as Android OS brings mobile development to the masses in an open source environment, so does ARK, with its software development kits, lean and stable Core, versatile plugins, and intuitive user interfaces. Simplicity is the cornerstone of ARK's core values.

3.2 Security

Today's world infrastructure brings with it risks and vulnerabilities. Blockchains mitigate these risks by achieving security through decentralization. Blockchain technology offers a unique blend of cryptography, peer-to-peer networks, and reward incentives. This results in users retaining their power while simultaneously removing weak points like data silos, honeypots, middle men, and various attack vectors. ARK has brought an advantage over Proof-of-Work networks like Bitcoin, allowing a network to remain secure even when small. This is achieved through ARK's unique recipe of the Delegated Proof-of-Stake consensus algorithm.

3.3 Speed

In order to achieve optimal decentralization, peer-to-peer networks like blockchains must trade off performance that is often enjoyed by centralized architectures. When millions of users trust one data source, that source can scale as needed to handle the load. When that trust is not an option, however, performance must scale down to accommodate additional independent data sources. ARK offers high-performance blockchain technology, proven through fast eight second block times on the ARK Public Network. This speed can be adjusted as needed for each bridgechain according to design requirements.

3.4 Scalability

The consensus mechanism ARK uses comes with built-in scaling advantages. Delegated Proof-of-Stake means that nodes conserve resources and scale up as needed to handle throughput demand. The network does not rely on every single endpoint to meet performance requirements, as end users are not running full nodes. Instead, they run lite clients and use their stake in the network to assign responsibility to nodes they deem worthy to secure and run the network. This keeps power in users' hands while simultaneously creating a highly scalable environment. ARK technology can also be customized to achieve higher performance through custom parameters, configurations, and network layouts. By enabling people to create their own unique blockchains, they receive a tailored solution while simultaneously contributing to an ecosystem of linked chains. This removes bottlenecks caused by the 'one chain, many solutions' approach.

3.5 Sovereignty

ARK believes that an organization, community, or other entity should be able to create a network of utility and governance without relying on external rules or limitations. This goes against the current trend, where one main blockchain network offers leased solutions that require interaction with that main network. This leased approach is not dissimilar to countries colonizing regions and then asserting dominion over them from afar, but it has never been known to work over the long term. Eventually, colonies seek sovereignty to forge their own future, and this rings true in distributed networks as well. The scaling limitations and imposed governance of 'one size fits all' blockchains will turn sour for disparate communities and organizations aiming to achieve and retain independence. Newly created blockchains can freely engage with each other and the ARK Public Network.

3.6 Support

Deploying blockchain technology that is easy to use and deploy still brings with it the need for easy access to support and help. With the ARK Public Network, community developers and organizations have a place to hone their skills and offer them to other entities who may need help deploying ARK technology in their selected destination. Community developers work hand-in-hand with the ARK team to evolve ARK's codebase. ARK Public Network delegates have become experts in ARK network maintenance and security. ARK community members and delegates launch services that enhance the toolset ARK offers. Incubators and consultancy firms can offer solutions and guidance to new projects. Choosing ARK as a blockchain solution means access to a large talent pool of support.

▲ 4 ARK Public Network

4.1 The ARK Mainnet

The ARK Public Network, also known as the "ARK mainnet" first came online on March 21st, 2017 [5]. At that time, 125 million ARK was created in a genesis block. The genesis delegates created to initialize the network were quickly replaced by live delegates who acquired community support in the form of votes and began securing the network. Shortly thereafter, block rewards were initialized in the protocol, rewarding forging delegates each time new transactions enter the ledger. The ARK mainnet operates independently of the ARK business entity, which simply releases code that the ARK mainnet delegates choose to either accept or reject. On the 28th of November 2018, the ARK mainnet upgraded from the now deprecated V1 codebase to the newly developed V2 codebase introducing a multitude of improvements to the network, developers, and end users [6] . ARK is among a very small group of teams in the blockchain space that has developed an entire blockchain based on experience of the founding members to address real-life business needs and expectations, rather than simply forking and modifying someone else's code.

4.2 Consensus Mechanism

A recent Fall 2018 technical paper entitled "The Latest Gossip on Byzantine Fault Tolerant Consensus" had this to say:

> *"Consensus is one of the fundamental problems and driving forces of distributed computing. It is important because of its role in State Machine Replication (SMR), a generic approach for replicating data that can be modeled as a deterministic state machine. The key idea of this approach is that node replicas start in the same initial state, and then execute requests (also called transactions) in the same order; thereby guaranteeing that node replicas stay in sync with each other. The role of consensus in the SMR approach is ensuring that all replicas receive and execute transactions in the same order. [7]"*

The ARK mainnet's consensus algorithm is known as Delegated Proof of Stake, or DPoS. This enables ARK to have a high-performance blockchain with block times of eight seconds, while simultaneously maintaining global decentralization and keeping the power in the users' hands. Holders of ARK use their wallets to vote for

delegates who secure the network, insert blocks into the ledger, and create new ARK. The ARK mainnet's implementation of DPoS is special compared to other DPoS projects, because its 51 forging delegates and 1 ARK = 1 Vote configuration solves two serious issues- namely, too much centralization due to insufficient node count, and delegate groups that can assert dominance over the network due to multivoting.

4.3 ARK Inflation Mechanics

Every eight seconds, two new ARK are created and awarded to the delegate that forged that block. Each block is forged by a delegate in turn, according to a randomly chosen slot within a round. With 51 forging delegates, each round lasts 408 seconds. Each round is also randomized to help combat attacks on delegates. If a delegate is prepared when it is their turn, a new block is forged and two ARK awarded. If a delegate is not ready to forge on their turn, it results in a missed block and two new ARK cannot be created. This incentivizes uptime. Barring missed blocks, the network has the capability to generate 7,884,000 ARK per year. The steady generation of a fixed amount of ARK means that the annual inflation rate steadily declines towards zero with each passing year. This is predictable and programmatically controlled, unlike fiat inflation [56].

4.4 Balancing Decentralization and Performance

The fewer nodes there are, the more risk of centralization exists. However, too many nodes can impact network performance. Bitcoin's slow block times, for example, allow for a very large number of nodes to reach consensus without much struggle. The ARK mainnet strikes a balance between decentralization and performance using 51 forging nodes. These forgers work in concert with what are known as relay nodes, which also maintain copies of the ledger and act as the contact points for lite clients.

Aside from node distribution, responsibility for decentralization is also assigned to ARK holders in the form of voting power. Each ARK wallet can execute a special transaction that assigns the weight of the ARK in that wallet to a delegate. This process does not transfer ownership of the ARK in the wallet to the delegate- it simply acts as a quantifiable show of support from the ARK holder that the delegate deserves to be in a top 51 position. As all of the ARK voting weight in the network is tallied up, it ranks the delegates to determine which should be allowed to forge new ARK and secure the network.

If a delegate begins acting erratically or dishonestly, voting weight can be assigned away from that delegate by the voters, allowing a different delegate to become one of the top 51 and fill the position. This creates a dynamic environment where the nodes who have the power to secure the network are in constant flux as community opinion shifts and as new delegates enter the space.

4.5 Preventing Collusion

Some DPoS architectures allow for multivoting [57]. This means that a wallet with 1000 coins can assign '1000 vote weight' to multiple delegates at once. This produced an interesting result where the entire list of delegates a wallet is voting for is public, and delegates could collude as a group and use social engineering to disincentivize holders from voting for anyone other than a specific group. This would essentially guarantee the delegate group's power and permanence in the network. With ARK, one holder who wishes to vote for multiple delegates would have to split that 1000 ARK into multiple addresses, each voting for a different delegate. This would in turn reduce the voting weight per delegate, and obscure the ownership of the wallets, preventing collusion on the protocol level.

4.6 Delegate Services

A delegate's role first and foremost is to secure the network, but to differentiate themselves, ARK mainnet delegates often pledge to run various services beyond securing the network, in a play to garner support and votes. These services may include development and testing, public resources and tools that utilize the ARK mainnet, faucets, bounty programs, outreach, art, games, media creation, events, research, and other unique services. This creates a dynamic landscape of options for voters, and voting plays a role in the future direction of the network. It also brings sustainability to the network, where multiple independent organizations form in the network that collaborate towards the common goal of network growth. The socioeconomic impact of this concept translates to any community that uses ARK technology for their blockchain.

▲ 5 ARK Network Uses

5.1 Role of the ARK Public Network

The ARK mainnet is not intended to operate similarly to other networks in the blockchain space, where multiple layers coexist. In some other public networks, a base communication layer with an incentivization protocol acts as a foundation for a decentralized application layer of some kind- be it storage, CPU-as-a-Service, tokenization, smart contracts, or some similar layer. While ARK technology is highly extensible through plugins, modules, and transaction types, the purpose of the ARK mainnet is to remain unbloated, lean, and fast. Using ARK products such as the ARK Deployer, other ARK based blockchains will appear in the ARK Ecosystem to handle specialized tasks as necessary. These newly created chains will then connect back to the ARK mainnet using ARK SmartBridge Technology. The ARK mainnet is intended to take on limited specialized functions only as needed, to facilitate the ARK mainnet as the hub of the ARK Ecosystem. The purpose of the ARK mainnet includes, but is not limited to, the below examples.

5.2 A Peer-to-Peer Cryptocurrency

At its core, the ARK Public Network hosts a global cryptocurrency called ARK that can be used for storing and transferring value, similar to Bitcoin. Bob can send Alice ARK much faster and cheaper than Bitcoin. Moreover, ARK can act as a unifying medium of exchange as needed within the ARK Ecosystem, due to its reach and liquidity. With the advent of the ARK Pay module as well as ever-evolving, intuitive lite clients, ARK is well positioned to be an effective network for both store-of-value and value transfer.

5.3 Medium of Exchange for ARK Mainnet Services

Delegates that reach forging status on the ARK mainnet may deploy services that either award or accept ARK. For example, a delegate running bounty campaigns can easily pay bounty recipients in ARK in exchange for providing value to the ARK Ecosystem through development, design, or outreach. Delegates that deploy or integrate their own platforms that use the ARK mainnet could accept ARK for their services.

For example, a large e-tailer could deploy a node and gather votes to enter forging status. They would then accept ARK on their e-tailer website for their wares, and offer big discounts to ARK holders and perks to their voters. When goods or

services are exchanged, the difference from discount could be offset using their delegate wallet, which generates new ARK. This would theoretically result in a type of 'discount faucet,' increasing their sales by simply running a forging node and accepting ARK, all without actually reducing margins. In this example, the ARK community benefits overall from the increased adoption and enjoys lower prices.

5.4 Convenience in Interoperability

It is reasonable to expect that ARK based blockchains will have use cases that benefit ARK mainnet users. These use cases can then appear in the ARK wallets in the form of a plugin. When ARK users wish to interact with that other use case, they can do so without leaving the ARK wallet. As the number of available use cases within the ARK wallet grows, so too does the convenience and utility of ARK. While newly created blockchains can also choose to list on fiat or crypto exchanges to give users access to tokens, ARK's approach reduces both the steps required and the risk for the end user, all while simultaneously preserving the bridgechains' sovereignty.

This mechanism can extend beyond bridgechain coins into bridgechain non-fungible tokens, for example, where NFTs become available for acquisition via SmartBridge. Imagine a video game launching a blockchain with a fixed number of specific types of weapons, items, and powerups on genesis. The assets could then be freely exchanged both within the bridgechain microcosm in question or via SmartBridge using ARK. Take notice that this arrangement of parallel chains reduces bloat on the ARK mainnet significantly if not entirely.

5.5 Liquidity for Small and Large ARK Bridgechains

When a brand new blockchain surrounding a community is formed, it usually creates an uphill battle to offer basic services for liquidity. They would need to get listed on reputable exchanges, which can take a long time and even incur listing fees and other red tape. The new community would also be subject to the inconvenience and risk of dealing with small fly-by-night exchanges, which are also subject to hacks and theft. Moreover, a successful exchange macrocosm only gives more power to these exchanges. In the long run, decentralized exchange is the best method, but it suffers from liquidity issues. ARK SmartBridge Technology can step in as a reliable first stage for decentralized exchange of assets and price discovery. The intertwining of ARK bridgechains with the overall ARK Ecosystem and ARK mainnet creates momentum that benefits everyone.

5.6 Payment Method for Plugin Marketplace

The modular structure of ARK technology creates the potential for a marketplace of plugins to grow, both in the form of Core plugins and lite client plugins. While most ARK technology is open-source and comes with boilerplate MIT-style licenses, this may not be true for all plugins. Both the ARK business entity and third parties have the ability to develop premium plugins which will be capable of generating streams of income in the form of licensing. License management and fees can be handled on-chain using the ARK mainnet and bridgechain registration, as well as other specialized transaction types. Similar to Android spawning a marketplace for third parties to generate revenue streams, so too can third parties generate similar streams using premium plugins and licensing. The medium of exchange for such a marketplace will be ARK. Plugin developers will be incentivized to accept ARK, as it will further the adoption of the very technology they utilize.

5.7 Payment Method for Delegate and Talent Marketplace

Similar to the plugin marketplace, there will be a growing need for talent and human services as the ARK Ecosystem evolves. For example, public networks launching new ARK based blockchains as well as commercial interests launching tokenless blockchains using the intuitive ARK Deployer may need assistance in handing off genesis delegates, customizing their chain beyond what the ARK Deployer can offer, or both. This becomes especially interesting with private enterprise chains. They may wish to distribute node ownership across both their internal organization and external operators in the interest of accountability. In this instance, delegates and delegate teams well versed in ARK technology can accept ARK coins from these enterprises, in exchange for running tokenless nodes and offering consulting services. It is even within reason that private enterprises may wish to outsource all node operations to delegates in the public marketplace, and simply distribute ARK to the delegates for the services of running tokenless enterprise chains.

6 Open Source Software

6.1 ARK Technology is Open Source

Open source software (OSS) is a type of computer software whose source code is released under a license in which the copyright holder grants users the right to study, change, and distribute the software to anyone and for any purpose. Anyone is allowed to create modifications of it, port it to new operating systems and instruction set architectures, share it with others, or in some cases, even market it. Free and open source software development models have made it possible to enable teamwork between previously unacquainted people who can help each other and follow a common goal [2].

6.2 OSS is Becoming the World Standard

According to a study by InfoSys, more than 78 percent of enterprises run on open source while fewer than three percent indicate they don't rely on open source software in any way. IT companies are in the phase of a big shift and transformation in the OSS arena with a healthy and positive mindset that open source software gains in strategic value. Big companies like Walmart, GE, Merck, Goldman Sachs, Google, and Facebook are also analyzing and moving towards open source. OSS can be seen as a first approach for enterprise architecture [2].

6.3 OSS Brings Benefits

ARK realized this from the start, and the result is one of the strongest open source communities in the crypto space. The benefits of the OSS model are clearly visible, with reduced costs, improved quality, and quicker time to market. If any developer or business wishes to develop solutions using ARK technology, there is always someone available and willing to help out. Due to the inherent nature of OSS, the code is more secure, as it is constantly exposed and under public scrutiny [2].

6.4 Building an Ecosystem

ARK prides itself in identifying as an *ecosystem*. An ecosystem can be defined as a community of living organisms and nonliving components. The living organism is ARK's strong, capable, and resilient community, growing every day worldwide. Non-living components are presented in the form of ARK projects, tools, products, and peripherals. ARK's work process is built around distributed best practices, which are promoted and used by GitHub and other big open source endeavors. ARK open source code is free for use under the MIT OSS license [2].

⬛ 7 ARK Core

7.1 About ARK Core

In order to prepare for the next generation of deployable DPoS blockchains, it became apparent that it was imperative to rethink the legacy code we inherited, and to move to a completely new codebase written from scratch. By monitoring the ARK V1 Public Network, and with the experience gained during development, several key elements were identified in the base design that could be optimized. Now, ARK has released the new codebase operational on the ARK Public Network as of late 2018 [2].

The new architecture has been completely rethought to decouple delegate forging activity, transaction pool management, and API interface on separate threads. Transactions will need to pass complete SPV (Simple Payment Verification) on a separate process or server before hitting the mempool, completely sandboxing the activity of the node against attacks [2].

ARK Core is a lightweight but very powerful codebase that functions as the base component of the entire ARK Ecosystem. Authored in TypeScript, the ARK Core was developed from the ground up with an extensive modular architecture to empower developers to modify, configure or extend all aspects of the codebase with ease. Now that all inherited legacy code is purged, the ARK business entity sees little future need for another bottom-up redesign. ARK's modular architecture will handle all further evolution of the ARK Core.

7.2 Dynamic Fees

The ARK Core uses a custom implementation of dynamic fees within a DPoS network model at the protocol level. This is not common in DPoS networks by any stretch, and is heralded as a large step forward for DPoS. The creation of a fee marketplace between users and delegates empowers the network to be frugal, resilient, and responsive. Dynamic fees benefit both the end users and the delegates that secure the network. The end user will benefit from the network accepting lower fees as delegates compete with each other. Transactions with a higher fee will be more likely to post faster. Dynamic fees will also assist the delegates by providing defense from potential attack vectors such as spam attacks. Delegates can also customize fees per transaction type [8].

7.3 Transaction Types

The ARK Core accommodates various transaction types, and has the ability to service new custom transaction types via ARK Logic. Below are some of the transaction types that are currently utilized within Core or planned for the future.

Transfer. The transfer transaction enables a user to broadcast a transaction to the network sending ARK tokens from one ARK wallet to another. This transaction type provides the utility of store-of-value and value transfer. Within this transaction type is also a special data field of 255 bytes called the *vendor field*, allowing raw data, code or plain text to be stored on the blockchain. The vendor field is also utilized in ARK SmartBridge Technology. The vendor field is public and immutable [59].

Second Signature Registration. This transaction type enables a user to add an extra layer of security to their address with the creation of a second passphrase, using mnemonic code for generating deterministic keys via BIP-39, creating an additional 12 words [41]. Once a second signature has been registered to a wallet, the owner of the wallet will then be required to input their primary and secondary passphrase when sending a transaction to the network [59].

Delegate Registration. A user or organization can register their address to become a delegate and secure the network. Upon accumulating sufficient vote weight, the delegate will begin forging transactions and receiving block rewards. The delegate assigns a custom name to their address to differentiate it from other delegates [59].

Vote & Unvote. A key feature of the ARK DPoS model is that each address can vote for one delegate of their choosing to secure the network. As a result, a vote and unvote transaction type is necessary to enable this functionality. Once an address votes for a delegate, funds can enter and leave the address as needed and vote weight adjusts automatically. Voting does not send funds to the delegate's ARK address in question- it only assigns vote weight [59].

Timelock. A transaction of this type acts as a simple logic function that restricts the spending of an amount of ARK at a specified address until a predefined future time or block height is met. This is useful for hash-based contracts and payment channels [59].

Multipayments. This type is designed to reduce the payload on the blockchain by enabling multiple payments to be combined together and broadcast to the network in a single transaction. This will benefit the end user and delegates by lowering transaction fees per payment and reducing congestion. Initially, the ARK Core will allow sixteen payments to be combined together within a single transaction. However, the number of payments per transaction can be scaled as needed [59].

Delegate Resignation. This transaction type will enable delegates to block potential voters from voting for them if they choose to withdraw their efforts in being a delegate. A non-reversible transaction can be sent to the network to indicate the delegate should no longer be included in any future forging rounds [59].

IPFS. This transaction type utilizes a special data field similar to the vendor field to store Interplanetary File System data on the blockchain. This provides an easy way to timestamp and optionally encrypt and verify files. This implementation of the IPFS transaction type won't allow storing data on the blockchain- for that, special IPFS nodes are needed [59].

Business Registration. This transaction type enables users and businesses to register on the ARK mainchain. More information on this is defined in section 11.5.

Bridgechain Registration. This transaction type requires the business registration first and gives users and businesses access to the ARK Deployer suite for bridgechain launching. More information on this is defined in section 11.5.

More transaction types can be implemented into Core based on community need, and the ARK Public Network can pick and choose which transaction types to

support, to keep the network lean and direct traffic to bridgechains as needed. Consult roadmap.ark.io for status updates on various transaction types.

7.4 Multisignature Protocol

The ARK Core will implement a multisignature protocol, or *multisig*, redesigned from the legacy version. ARK's multisignature implementation will require multiple keys to authorize an ARK transaction to be broadcast to the network. This implementation will enable users, developers and businesses to divide responsibility of possession of ARK tokens. A practical implementation of multisig can be found in large Bitcoin exchanges, where a trusted group of individuals controls keys to one single wallet/address. For example, an exchange controls a cold wallet containing ARK. This exchange could implement a '3-of-6' multisig which would give six separate passphrases for one address. This address will only be allowed to send transactions if three out of six keys sign, as a way to distribute responsibility of holdings while increasing security and minimizing risk.The pending ARK multisignature implementation is quite similar to the way Bitcoin multisigs work, using Schnorr multisignatures [43].

7.5 ARK Core CLI

As of v2.2.0, Core has become a Node Version Manager (NPM) module that can be installed and interacted with globally. A built-in Command Line Interface (CLI) is now available as well. NPM is the world's largest software registry, and installation of Core is now effortless for anyone regardless of technical background. The CLI is an essential tool that enables any node operator to update, manage, or monitor their node installation without the need for any external programs. ARK Snapshot manager is also integrated into the CLI. All ARK-based bridgechains will also be able to take advantage of the incredibly powerful ARK CLI toolset.

7.6 Core Plugins & Modular Architecture

ARK Core is split into multiple packages using Lerna to manage their development and publishing. The benefit of this approach is that it is easier to focus on smaller parts of the whole system, with each as a standalone package. Each part of the core can be replaced by custom implementations. For example, a custom core-logger-logstash package could replace the default logger without affecting the stability of other components. All of these plugins are interconnected via the Core Plugin Manager package, which functions as a container to hold all of the instances that are shared across plugins [2].

The plugin manager allows us to provide different Bootstrap processes for things like starting a relay node or a forging node. The plugin manager accepts two parameters, the path to a folder that contains a plugins.json file, and an optional parameter that can contain options like including and excluding plugins from the Bootstrap process or plugin-specific options that are not available from the standard configuration file [2].

A key tenant of ARK's extensibility lies in this plugin architecture. Future plugins released by the ARK business entity as well as third party plugins can integrate into Core, adding new benefits. When deploying a custom blockchain, use case plugins can be developed and integrated without affecting the stability of the existing code.

7.7 ARK Webhooks
The webhook API has been integrated into ARK Core to enable developers to listen to specific events from the ARK blockchain. Webhooks provide other applications with real-time information without expending resources unnecessarily. As ARK grows, traffic on the network will increase. Utilizing webhooks removes the need to poll the network for data which can cause network stress. On average, 98.5% of polls are wasted and increase the workload on the server, making webhooks much more efficient. Based on user specifications, the webhook notifications will be sent out on every block update, including transactions sent, transactions received, and other timing events built on the ARK blockchain [9].

7.8 ARK Core Docker
ARK Core is now available for Docker, the industry standard for packaging applications into a container. This will give developers another tool to quickly install and run an ARK node. Using a Docker image, all dependencies such as the language runtimes and libraries are combined within the container, making an all-in-one node installation much easier [10].

7.9 ARK Snapshot Manager
An all-new local snapshot system has been developed, allowing node operators to use their copies of the database when needed. When starting a new node or rebuilding a node due to errors, local copies allow for fast and safe synchronization. The ARK Snapshot Manager provides simple commands such as *dump, restore, rollback, truncate,* and *verify*. The ARK snapshot manager has been integrated into the ARK CLI since the release of ARK Core 2.2.0.

7.10 ARK Utilities

ARK Utilities is a separate library providing common functions for working with data and performing common tasks while simultaneously increasing performance across the entirety of ARK Core. By introducing this new dependency layer, many third party dependencies can be replaced in Core with elements of the ARK Utilities library. Additionally, a common API can be provided. This allows developers to swap out or make changes to the implementations as they identify performance issues and other shortcomings, all without affecting the API. Extensive real-world testing has proven ARK Utilities to offer multi-fold improvements as high as 12x over other libraries such as Native and Lodash [11].

▲ 8 ARK Peripherals

8.1 Expanding on Core

Now armed with a lean and powerful Core, ARK can expand its value proposition through useful peripherals, which include software development kits (SDKs), external products, open source projects, branded plugins, and more. These peripherals combine to deliver a family of solutions that come with any newly deployed ARK blockchain. Through sharp vision and community support, anyone who needs a blockchain will have everything they need right out of the box.

8.2 ARK Software Development Kits

Using ARK SDKs, developers can employ the programming language of their choice to build applications utilizing the ARK blockchain. Each implementation is split into two sub kits: *Client* and *Cryptography*. Client sub kits help developers fetch information from the ARK blockchain about its current state, such as which delegates are currently forging, what transactions are associated with a given wallet, and so on. Cryptography sub kits, by contrast, assist developers in working with transactions, such as signing, serializing, deserializing, and the like.

The following SDKs are currently available:

> *C++*. C++ is widely used in embedded systems software engineering. The addition of C++ pushes ARK further into the world of IoT as it can be run on microcontrollers such as Arduino and Raspberry Pi [12].

> *.NET*. The .NET motto is *Any developer, any app, any platform!* As such, this framework is a very popular platform in corporate settings. It is the perfect tool for startups and hobbyists who are just starting out with ARK and would like to jump right in [13].

> *Elixir*. Elixir takes advantage of the Erlang VM, which is known for running low-latency distributed and fault-tolerant systems, while also being successfully used in web development and embedded software domain [14].

Go. GoLang is an open source programming language developed by Google and designed for building fast, simple, and reliable software. It is not about theoretical concepts such as monads and virtual inheritance, but more about hands-on experience [15].

Java. Java is a general-purpose computer-programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. With ARK's Java SDK design, it is easily to re-use Java Crypto and Client packages to integrate into popular frameworks such as Kotlin, Groovy and Scala. [16].

Javascript. Javascript is an object-oriented computer programming language commonly used to create interactive effects within web browsers. Javascript is one of the most widely used languages on the Web, and the ARK Core is written in Typescript, a more stringent flavor of Javascript [17].

PHP. PHP is an extremely popular open source scripting language that is well suited for web development and can be embedded into HTML. PHP is used as a server-side programming language for over 80% of working websites [18].

Laravel. Laravel is an important member of a new generation of frameworks [19]. It is a free, open source PHP web framework with expressive, elegant syntax intended for the development of web applications [20]. Laravel is extremely popular with developers ranging from hobbyists to enterprise level. Laravel is very highly ranked according to Github [44].

Symfony. Symfony is a set of reusable PHP components and a PHP framework for web projects. It allows you to speed up production and maintenance of your PHP web applications and ends repetitive coding tasks. This also benefits developers as they can also add their own modules. Symfony is popular in the enterprise space [21].

Python. Python is a great starting language as it's widely taught in universities and used for working with beginner and IoT-friendly devices such as the Raspberry Pi. Python is powerful and fast,

plays well with others, runs everywhere, is friendly and easy to learn, and most of all, it's open to everyone [22].

Ruby. Ruby is a dynamic, reflective, object-oriented, general-purpose programming language. It supports multiple programming paradigms including functional, object-oriented, and imperative. It also has a dynamic type system and automatic memory management [23].

Rust. Many companies both large and small use Rust in production for a variety of tasks. Those tasks include command line tools, web services, DevOps tooling, embedded devices, audio and video analysis and transcoding, cryptocurrencies, bioinformatics, search engines, Internet-of-Things applications, machine learning, and even major parts of the Firefox web browser [24].

Swift. Swift is a powerful and intuitive programming language for macOS, iOS, watchOS and tvOS. Writing Swift code is interactive and fun, the syntax is concise yet expressive, and Swift includes modern features developers love. Swift code is safe by design, yet also produces software that runs lightning fast [25].

Wolfram. The Wolfram Language leverages built-in computational intelligence that relies on a vast depth of algorithms and real-world knowledge carefully integrated over three decades. Wolfram is heralded as the first true computational communication language for humans and AIs. Wolfram is adding full read and transactional write support for ARK [26].

RPC. The JSON-RPC compliant [45] SDK was created to aid organizations with the integration of Ark in their existing RPC based infrastructure when extenuating circumstances make using the ARK Public API less than ideal. All operations provided by the JSON-RPC can be performed using the ARK Public API. [27].

8.3 ARK Test Suite

Most software developers are aware of how hard it is to get full test coverage over different testing phases that must take multiple stakeholders into account [58]. Now add blockchain mechanics to that recipe, and think about how to test distributed systems, their mechanics, security, block propagation, transaction management, transaction pool handling, fork management, client API- things get dicey.

With these challenges in mind, it was paramount to pick the right tool that is flexible and powerful enough. Upon assessing the market for options, it was decided that the Jest Framework best suited ARK as the base testing framework. Jest was developed and is used by Facebook to test all of their JavaScript code including React applications. Jest is also used by Airbnb, Twitter, Pinterest, Instagram, and Oculus [2]. We are establishing a common base for developers, delivering the best possible tools, like powerful mocking, snapshot testing, built-in code coverage, and zero configuration. ARK Test Suite also makes cross team collaboration smooth with testing appearing uniform across different sections of code. By doing so, we deliver valuable implementation examples, enabling newcomers to learn and understand the existing code.

8.4 ARK Explorer

The ARK Explorer is a fundamental tool, designed and developed from the ground up, using lean and fast developmental frameworks Tailwind CSS and Vue.JS [38]. Sporting an aesthetically pleasing design, the ARK Explorer boasts features such as light and dark mode, multi language support, and token price tracking.

The ARK Explorer provides the user with critical data such as viewing the latest transactions and blocks, searching for wallet addresses and transactions, viewing wallet address rankings, and monitoring delegates for visibility on network state.

8.5 ARK Desktop Wallet

The ARK Desktop Wallet is a multi-functional application written from scratch using VueJS and TailwindCSS, implementing the latest Electron framework [30]. The structure of the public and private key generation follows the same specification as Bitcoin, with the exception of using BIP-39 passphrases for end user ease of use. A custom implementation of BIP-32 for Hierarchical Deterministic Wallets is provided to ARK users. The ARK Desktop Wallet supports multiple transaction types with the added benefit of empowering the end user to determine transaction fees with the introduction of dynamic fees. Customization

was an important factor during development to ensure that developers, businesses, and end users could personalize the wallet experience for their own requirements. Because of this, the Desktop Wallet is becoming modular with the advent of wallet plugins. Bridgechains can implement use cases directly into the ARK Desktop Wallet, and third party developers can enhance its features. With support for multiple ARK networks enabled, the ARK Desktop Wallet is invaluable within the ARK Ecosystem.

The ARK Desktop wallet is a lite client, working in tandem with ARK DPoS to deliver a seamless experience. Users can launch the wallet and interact with the blockchain immediately, with no need to sync. The wallet is also compatible with the Ledger Nano S hardware device, offering passphrase management in a secure sandbox. The ARK Desktop Wallet allows all bridgechains to be added directly for seamless chain management, automated by bridgechain registration. All bridgechains also gain the advantage of Ledger Nano S support via the ARK desktop wallet.For the ARK Public Network, the wallet is integrated with Changelly, where users can acquire ARK using other cryptocurrencies and fiat from directly within the wallet.

The ARK Desktop Wallet is available on Windows, Mac and Linux operating systems.

8.6 ARK Mobile Wallet

The ARK Mobile Wallet is a hybrid application that uses the same codebase for Android and iOS which helps with coordinated development. The ARK Mobile wallet was created using Ionic framework and ARK's TypeScript API to interact with the network via mobile device [31]. The wallet supports multiple transaction types, with the added benefit of empowering the end user to determine transaction fees via ARK's dynamic fee implementation.

The ARK Mobile Wallet is available on Android and iOS operating systems.

8.7 ARK Pay

ARK Pay is a simple open-source library that provides merchants with the ability to easily accept ARK as a means of payment in online stores. ARK Pay is an official ARK supported plugin developed in JavaScript [32]. ARK Pay provides developers with a plug-and-play module to allow easy implementation of ARK as a payment method on websites and within web-enabled applications. ARK Pay also utilizes a

customized URI scheme, enabling the auto-fill of wallet parameters via clickable link or QR code.

The next iteration of ARK Pay will also feature a backend for a better transaction management experience. The custom developed backend will have verification and order processing on the server side instead of polling the blockchain via public API. It will also become easier for ARK bridgechains to have their own ARK Pay plugin up and running in no time, supporting their own blockchain by simply inputting their own network parameters.

8.8 ARK Deployer CLI

ARK Deployer CLI is a lightweight deployment script for creating your own ARK-based blockchains. By utilizing the ARK Deployer, developers can create their own bridgechain in a matter of minutes. ARK Deployer is just the first step in building a more robust ecosystem that will be user friendly and will feature the same caliber of user experience that is to be expected from ARK. ARK Deployer configures, deploys and integrates the following:

> Deploys ARK node in auto-forging mode on a single computer or server, with your chosen number of forging *genesis delegates*. Genesis delegates act as initial placeholders until node operators in the field replace them. Custom parameters can be configured such as block times, transaction fees, block rewards, transactions per second, and so on. Bridgechains operating under the right conditions can theoretically reach thousands of transactions per second.

> Deploys ARK Explorer that is already configured and talking with the installed ARK node. This clones, configures, installs and integrates ARK Explorer with the ARK node.

> Configures ARK API for the developer to start exploring, hacking, and developing solutions based on ARK technology [33].

8.9 ARK Deployer GUI

In alignment with ARK's master vision of giving as many people as possible the power of blockchain technology, the ARK Deployer will be skinned with a graphical user interface in 2019. This will allow developers to visually configure their blockchain parameters and selected plugins without the need to interact with the

Deployer CLI. Over time, complex processes will become simpler, and creating custom blockchains will become akin to designing a website with WIX or Squarespace. Anyone who needs a blockchain can focus on their needs and leave the heavy lifting to the Deployer backend. The Deployer GUI can also access a marketplace of plugins and other ARK technology to add functionality to a chain.

▲ 9 ARK Logic

9.1 Bitcoin Scripts

Bitcoin removed central authorities from the process of transferring money over the Internet. Before Bitcoin, it was simply not possible to digitally transfer wealth online without some form of centralized intermediary [34]. Bank transfers required banks, and credit card transactions required credit card companies and merchant processors. Digital currencies relied on centralized servers with trusted parties to store account information, transaction data, and often, assets backing the value of the currency.

Now, with cryptocurrency, you can send funds to anyone else on the network without using a centralized authority acting on your behalf. In the beginning of Bitcoin, Satoshi had plans to go beyond simple send and receive functions using its programming language known as 'Bitcoin Scripts [35].' This would have given Bitcoin the capability of becoming truly programmable money. An example of Scripts in action would be multisig, where multiple users must sign before funds are released. Bitcoin has since pivoted away from complex on-chain logic.

9.2 Ethereum Virtual Machine

Ethereum took up the torch on the programmable money concept, and expanded on the concept further- much further. While Bitcoin Scripts could be seen as the punch-card computer programs of old, Ethereum was seen as the first 'operating system' that directly addressed virtual money in a decentralized environment. Ethereum Smart Contracts ran within this operating system, known as the EVM, or Ethereum Virtual Machine. Using a unique new language called 'Solidity,' functions ranging from simple 'if-then' statements all the way up to entire applications could execute, and with far less technical acuity than is required with Bitcoin Scripts. Ethereum Smart Contracts were a large step in the right direction. The more functions programmable money can handle by itself, the more autonomous it can become [36].

9.3 Smart Contract Example

A basic example of a Smart Contract is something seen hundreds if not thousands of times throughout the last few years- the ICO, or Initial Coin Offering. The Smart Contract in this example is rather simple. An organization accepts a liquid asset (Ether) at a specific address, and when Ether arrives, the Smart Contract

automatically sends a new asset back to the source address at a given fixed exchange rate. This continues until a specific limit is reached or a specific amount of time has elapsed. It's all handled autonomously by the Smart Contract. The organization then uses its newly acquired Ether to conduct operations, while the holders of the new asset are free to trade it with other parties or use it for products and services.

9.4 Smart Contract Immutability

Even Smart Contracts as simple as the example above have been identified to contain critical bugs in the past, and as their complexity grows, so do the frequency and potential impact of these bugs. A Summer 2018 article cited a code auditor that determined that twenty-five percent of all smart contracts contain critical security issues [37]. While vulnerabilities and critical flaws can be patched in normal software systems, Smart Contracts are completely final and cannot be modified once deployed. This means the first and last line of defense lies with the Smart Contract authors and pre-auditors, where lack of understanding of Solidity, hasty deployment, and inability to react quickly to new information all pose a substantial threat to safe Smart Contract execution.

9.5 Smart Contract Bloat

Standard Smart Contract architecture where developers deploy versatile and complex applications tend to require a Virtual Machine of some sort, similar to the EVM and others. This essentially provides the 'runtime engine' in which the applications reside. Virtual machines must run a variety of applications, and this usually results in a bloated system that requires heavy resources to run simple tasks. ARK is deploying solutions using custom transaction types and plugins, so specific goals can be reached with far less overhead, making solutions built with ARK technology far more scalable.

9.6 Smart Contract Complexity

Another problem with Smart Contracts lies within their complexity. The Solidity language utilizes a multitude of granular functions to build complex applications. However, this can result in awarding too much raw power to the developer, who may inadvertently introduce the potential for exploits into their program. By distilling common business logic into 'building blocks' that can be assembled in a more controlled environment, customized results are attainable with far less risk. The goal of Ethereum was to expose more people than ever before to the power of decentralized computing within cryptocurrencies. ARK intends to do this while also

realizing as more people become capable, more safeguards must be in place to prevent errors, all without withholding power from developers.

9.7 ARK Logic as a Solution to Smart Contracts

From the start, our intent was to provide an answer to the Blockchain Trilemma and reduce the well known limitations of blockchain technology. Some of these solutions are baked into SmartBridge technology, allowing for greater flexibility and scalability via an ecosystem of linked chains with specific use cases. Aside from the Blockchain Trilemma, however, we saw the above issues with Smart Contracts and wish to address them as part of our vision. We see Smart Contracts as small automation engines being executed in black boxes, that lack the modern pace of development and flexibility, and developers need to learn an additional language to deliver them.

Our solution to this is to deliver more than just automation and distributed relay execution. We want to give organizations the power to develop their own application logic, the way they are already used to doing it, by using existing tooling and developing normal applications that can be deployed on our blockchain infrastructure via the modular architecture of plugins. A plugin is a normal Typescript application that has the full power of blockchain, with all of the expressive capabilities of using a common programming language. It acts as just another application that can be deployed and maintained via blockchain mechanics, running on our core blockchain engine. By developing a plugin, you are able to add new tables, storage options, web servers, and complete graphical interfaces running and using the Core technology as a driving force.

9.8 ARK Logic is Flexible

Being able to deliver the power of adaptation and flexibility is one of the first steps to deliver mass adoption and attract more developers to build using ARK technology. Smart Contracts will evolve into business applications running on ARK bridgechains. In addition to plugins delivering new ARK functionality, developers can fully customize their blockchain behavior, with a perfect example of this found in the ARK Deployer. They can define custom behaviour of the DPoS mechanism, adjust block time and TPS, change number of delegates, and adjust the fee mechanics and block rewards. Everything is fully flexible.

On the transaction level, we introduced the new concept of adding custom transaction types that still follow the blockchain processing rules, but can be custom tailored as needed. Custom transaction types, unique plugins, and a fractal

network of interconnected bridgechains handling specific use cases all combine to maximize flexibility for developers.

9.9 ARK Logic is Scalable

Scalability, being part of the Blockchain Trilemma, is solved with SmartBridge Technology and ARK Logic. Although some other blockchain projects are aiming to act as a global supercomputer, we don't want to fit everything into one black box. Separation of concern is already a well established pattern in software development, and we applied the same ideals while addressing the scalability challenge. If a business or organization has a need for specific processing power, custom applications that need faster confirmation times, or oracles that address a specific business process, the best approach is to launch and configure an application-specific chain and implement a module addressing the needed business logic. By doing so we gain in three ways:

> Strain on the main ARK network is reduced, as resource requirements are moved from mainnet to bridgechain

> Stability is improved, as a bridgechain can be run in an isolated environment, free from the bloat of external operations

> Upgrades become easier as logic can be modified and improved, in contrast to the finality of Smart Contracts. The application can scale provided consensus is reached.

Moving processing logic from mainnet to bridgechain also addresses other known concepts such as sharding or payment channels, thus closing the horizontal scalability issue. Both of the approaches are achieved via bridgechain launch and its customization.

Scalability also walks hand in hand with interoperability for ARK. With the introduction of bridgechains we gain clear separation of concerns, while moving business logic to the application-centric bridgechains.

9.10 ARK Logic is Simple

We addressed the Blockchain Trilemma issues with knowledge and experience gained from real work usage on the ARK mainnet for more than two years, and with valuable feedback gathered from companies developing their projects using ARK technology. We are looking at all of the possible use cases of blockchain

technology, and we are addressing them with a lean and stable core, a vast array of SDKs, an intuitive blockchain deployer, modular technology via plugin infrastructure, custom transaction types, and interoperability via SmartBridge Technology. We support all of this with extensive and thorough documentation, guidebooks, tutorials, code examples, and help from community developers. ARK Logic components such as modular plugins and TX templates will combine with the above elements to make creating and deploying decentralized applications extremely simple, but ARK technology is far from basic. The K.I.S.S. approach of ARK Logic will allow anyone to create or enhance their project in the most efficient and standard way.

▲ 10 SmartBridge Technology

10.1 The Need to Interoperate

The need for interoperability is a serious issue, and ARK has had a major impact in this field. The SmartBridge approach allows ARK to bypass one of the most common issues surrounding different blockchains, which is the isolation between each one. The communication between different coins/blockchains is currently controlled by centralized exchanges in the form of asset transfer only. ARK is looking to change this by allowing asset and data transfer without the need for custodial third parties.

SmartBridge communication can be defined in two ways:

> *Protocol-Specific SmartBridge.* This represents communication between various chains based on ARK Core technology that live and operate within the ARK Ecosystem's network of bridgechains. This is also known as bridgechain communication.

> *Protocol-Agnostic Smartbridge.* This represents communication between blockchains that use different consensus mechanisms, tokens and protocols, for example Bitcoin and others. This is also known as cross-chain communication.

10.2 ARK-ARK SmartBridge Mechanics

Bridgechain protocol defines a new communication layer targeting ARK-based application-centric blockchains. Communication between bridgechains will bring more than just token swaps (ability to exchange data, information, bridgechain validation) and will define the groundwork for the businesses and projects to communicate via the new protocol. More on this will follow in future documentation including a specific ARK Improvement Proposal defining the bridgechain protocol in detail. Protocol realization was recently made possible with the release of the brand new Core v2, and by enabling functions supported by ARK Logic.

Bridgechain protocol will be introduced in the form of a new Core module *core-bridge.* The core-bridge module operates hand in hand with the new bridgechain registration transaction type delivered by the ARK Deployer, while still

carrying proof of trust/ownership of the originator of the registration transaction. Bridgechain registration means that any new bridgechain will need to be registered via our mainnet. The ARK Public Network will act as a proxy, main highway, and decentralized guard to interchain communication.

ARK has been upgraded for event triggering with the use of webhooks and basic event emitters. Events are used inside the Core to trigger blockchain actions and the delivery of webhook payloads. Additionally, custom plugins can utilize the event emitter package to trigger their own actions in response to blockchain events. Conceptually, this feature is similar to the *Hooks* implementation in WordPress [49], as well as the lifecycle hook access provided by Javascript frameworks such as Vue and React [50] [51].

A primary difference is that due to the need for strict protocols around blockchain data creation and retrieval, events are strictly reactionary. Core events are not capable of changing data at runtime. The *transaction applied* event, for instance, passes a complete transaction instance, not raw transaction data that can be altered in the style of a WordPress filter. Another way to think of the event API is in the context of a *publish-subscribe pattern* [52]. In this pattern, ARK Core packages can act both as publishers and subscribers of events.

Bridgechain protocol transactions enabling coin transfers will need to be confirmed on all three levels: the sending blockchain, ARK mainnet, and the receiving blockchain. The bridgechain protocol logic will be replicable, meaning that any bridgechain is able to act as a self-governing mainnet, thus making a horizontal connection through the spider web of blockchains and enabling exit via ARK mainnet.

10.3 ARK-ANY Smartbridge Mechanics

A community project called *ARK Contract Execution Services* otherwise known as ACES has shown everyone that it is possible to have two-way transfers between ARK and Bitcoin, Litecoin, and Ethereum, including issuing Smart Contracts from ARK to Ethereum, regardless of the underlying protocols. ACES can adapt to any blockchain as needed [54].

Communication takes place through a special data section called vendor fields. At 255 characters, each transaction can be used to send text, instructions or code. This can also be used as hashing functions or even trigger events such as Smart Contracts on other blockchains.

Intermediary nodes known as *encoded listeners* comb through this data for tasks to perform. These encoded listeners can be programmed and run however the operator sees fit, including running an exchange pool similar to ShapeShift or Changelly. Competing encoded listener node runners can launch ACES nodes for various coins, creating an encoded listener marketplace [48].

ACES is not a fully decentralized solution, even though it can result in multiple interaction points between two chains that are independently operated, providing redundancy. It is worth noting, however, that aside from handling other blockchains, ACES can handle communication between ARK-based chains as well. ACES can be used while the decentralized SmartBridge Technology between various ARK-based blockchains is developed, and other blockchains or tokens that wish to migrate to ARK can do so via ACES token bridge. ACES is currently undergoing upgrades due to the recent ARK Core redesign, and aspects of the ACES approach are carrying over in the Core itself. An example of this approach that uses the plugin/module implementation is when ARK technology and HyperLedger Fabric were integrated. The plugin-enabled execution of HyperLedger SmartContracts functions via ARK SmartBridge by using the vendor field as an interface [53].

Focus will be more thorough on cross-chain capabilities after the initial ecosystem is built with seamless bridgechain communication via the new bridgechain protocol. For now, the focus will be on building the ecosystem further and delivering promises of interchain communication among ARK-based blockchains.

⏏ 11 ARK Business Strategy

11.1 Business Strategy Introduction

The Gartner technology hype cycle illustrates a point of an *Innovation Trigger* which leads to a peak of *Inflated Expectations*. Afterwards, a *Trough of Disillusionment* forms followed by a *Slope of Enlightenment*, to rest on the *Plateau of Productivity* [39]. Applying this cycle to blockchain technology, we believe the technology is in the process of exiting the Trough of Disillusionment, making this the perfect time to focus more heavily on executing plans to build a customer base, gain strategic value, and create new revenue streams for the ARK business entity.

The best way to move forward is to deliver solid and easy-to-use technology that will enable new use cases and disrupt the existing ones. The key challenge here is to provide the tools and technology that makes this an easy switch, and this is where ARK's main vision and motivation comes from. We will continue improving and implementing new features with input from the community and wider audiences. Working together by listening to and understanding our early adopters will help us improve and deliver on our promises using ARK's technology stack.

11.2 ARK SCIC Business Entity

ARK is currently incorporated in France as a cooperative society known as an SCIC (Société Coopérative d'intérêt Collectif). It is the first of its kind in the crypto world, and one of the first blockchain projects to incorporate in the EU [40]. ARK has also met with the AMF, which is similar to the SEC, and maintains a close relationship with them for regulatory compliance. ARK also has close ties to the French government and has contributed to Article 26 of the Loi Pacte and both Parliament reports on blockchain and cryptocurrency [46] [47].

11.3 ARK Team

The ARK team, also known as the *ARK Crew*, is decentralized throughout the world and has no main office. Team members come from the United States, France, Spain, Brazil, United Kingdom, Germany, The Netherlands, Slovenia, Finland, Bulgaria, Ukraine, and others. The ARK Crew is determined to change the world by giving everyone accessibility to the awesome power of blockchain. We have been expanding and hiring more talent regardless of market conditions, and we are in possession of multiple years' worth of working capital in various cryptocurrencies.

11.4 Moving to a Customer & Value Centric Approach

The initial phase of ARK's business strategy was to develop a solid foundation of technology with which custom solutions and applications can be built by others. With a newly reimagined Core and large family of peripherals, ARK can now begin its shift towards catering to customers, or the organizations and open source communities that intend to use the technology. ARK will do this by using its own tools and ARK Logic templates to expand on its current offerings and attract developers in certain industries of interest. Once this takes place, the ARK business entity can focus on providing true value to those that need application-specific blockchains. ARK's toolset will always be versatile for any use case, but the ARK business entity intends to offer help and guidance for specific industries through tools and features that are a bit more tailored. This will reduce the barriers to entry even further for those industries.

The value-centric proposition is not the same as the API-centric, which is a technical solution. More precisely, the value proposition describes what value you offer to the customer and why the customer should buy it. The API describes how you provide value to the customer [42].

The value-centric approach is important for organizations already running their business that want to improve their product offerings, or add new blockchain-enabled features or products. This is where ARK technology comes into play as a solid choice. We will focus on this aspect and help businesses improve their technology by adding new value propositions and solving some of their existing customers' pains with industry-tailored tools. Any remaining gaps will be filled by the community and ARK digital marketplace as needed.

11.5 Transformation Into a Digital Marketplace

Building the ARK Core around component based architecture brought much more than just a modular and flexible codebase. Core plugins are the framework to introduce a new era of business-oriented distributed applications. Organizations can develop business applications on our already established and running blockchain platform by using plugin development tools and ARK Logic. An ARK plugin can be anything from a simple API expanding and enabling storage of additional data on the blockchain, to a brand new HTTP server with custom underlying logic, delivering new application interfaces and support for any kind of business related challenges. Developers can use our already available SDKs,

libraries, and utilities, so they can focus on business application development. ARK plugins can be developed in JavaScript and Typescript.

Every plugin can introduce its own licensing and support conditions. A plugin license can be stored on the ARK mainnet in the form of a transaction. Some plugins will run solely on bridgechains and some will be part of the mainnet only as needed. For the plugin to reach mainnet, a wide consensus between public delegates is necessary.

This brings us one step further to the introduction of a digital marketplace- a convenient destination to discover, buy and sell applications, services and solutions built with ARK's technology stack. The marketplace will make it easy to find and publish new solutions built on top of ARK technology. Its main purpose is to connect service providers, developers, startups and larger enterprises. To enable this, new transaction types will be introduced for the ARK Public Network.

Transaction types will be created for business and bridgechain on-chain registration. This will enable businesses to register on the ARK mainnet and further develop ARK plugins that can be traced back to the business registration transaction, which will contain more details about the company. This will also solve the pressing matter of bad actors who wish to disseminate malicious code posing as well-established developers.

> *Business Registration on ARK Public Network.* An individual, team or company will be able to issue a business registration transaction in the same way a delegate registration transaction is issued. The proposed fee for this transaction should be high enough so only serious projects will take this on. With this transaction, more company or project details must be provided such as website, github, VAT ID if applicable, contact email, etc. This transaction will serve as an entry to the next scenario, where the registered business on the ARK Public Network can request a bridgechain launch via the ARK Deployer GUI.

> *Bridgechain configuration on ARK Public Network via ARK Deployer.* An address that is registered as a business or organization can send a bridgechain registration. This will serve as an input to the ARK Deployer as it would use this address to further generate the chain specifications such as genesis block, initial wallets and

passwords, mainnet, devnet and testnet specifications. This establishes authenticity for the bridgechain, opening doors to certain strategic value opportunities within the ARK ecosystem that will not be available to an unregistered chain, such as the *Powered by ARK Program*, currently in development for 2019.

Entry into the Powered by ARK Program via bridgechain registration simply means that the team behind the project is serious and capable, and that the project was assessed and evaluated by ARK community and team. This can also be read as partnership and give a green light to proudly use the 'Powered by ARK Core' logo, as well as official listing on ARK mainnet and peripherals. Being listed on the ARK mainnet triggers bridgechain awareness, visibility, and above all, capability to communicate. The ARK mainnet will act as a proxy and a decentralized guardian for interchain communications.

New transaction types and plugin deployment using ARK Logic go hand in hand with the new functionalities of the ARK Deployer. Deployer serves as the primary vehicle for building, launching, and managing blockchains. The deployer user can select and register a new bridgechain, and preselect the set of modules and plugins included in the bridgechain launch. This will enable users to launch custom bridgechain specifications already adapted to specific industries of interest, and customize their chain for any use case with third party tools and plugins.

11.6 Industries of Interest

The ARK business entity will soon start using its own tools to tailor solutions and add-ons for specific industries. This means that soon, players in these industries will have ready-made tools out of the box to utilize in deploying their blockchain solutions, using ARK Logic. As more entities in these fields use ARK technology, the building blocks can be refined and expanded, producing further ease of use for whoever is next in line. The ARK business entity, after creating such industry-specific toolkits and ARK Logic templates, will start facilitating usage of the solutions among organizations, and form strategic partnerships within these sectors as needed. The ARK business entity will be focusing on four industries of interest to start: Gaming, Internet-of-Things, Government, and Supply Chain Management.

Gaming. Blockchain has the power to completely change the way that developers approach game design. Blockchain can also

elevate the way that players interact with gaming ecosystems. Decentralized infrastructure enables immutable ownership of in-game digital assets, completely transforming the control and flexibility that players currently have in centralized gaming environments. Further to this, issues with hacking, duplication and theft are mitigated through the encryption provided by blockchain networks, all leading to massive increases in security for both gaming infrastructure and players' digital possessions.

Exchange of assets between games may also be enabled with a common game asset protocol built on a network of ARK blockchains, along with exchange for non-game digital assets and currencies. Non-fungible tokens allow for serialized, uniquely identified, transferable in-game assets.

Blockchain transforms in-game mechanics and processes in a way that promotes trust and accountability within gaming environments. A re-imagined system for payments and monetization could lead to huge cost savings for both developers and gamers, leading to increasingly fair and optimized in-game economics.

By utilizing ARK blockchain technology, the gaming sector is able to tackle key challenges related to security, ownership and fairness. Along with this, faster and more flexible payment systems, new ways of building credibility, and improved transparency mean that new opportunities throughout the industry can be leveraged.

Internet of Things. As the IoT industry continues to grow, it's increasingly plagued with issues surrounding security, poor connectivity and slow performance, limiting its ability to fully penetrate the commercial and industrial sectors. Industry leaders are crying out for a scalable solution that will enhance security, improve network performance and reduce the reliance on centralized cloud servers, and that's where blockchain technology shines.

With its innate immutability and decentralized nature, blockchain is the perfect fit for IoT. It addresses the key challenges that the IoT industry faces, from device security to the authentication and encryption of information.

A decentralized network means that the risk of IoT devices being compromised via a single point of failure is mitigated, and the reliance on expensive, centralized data centers is significantly reduced. Moreover, a lean, scalable network capable of supporting millions of connected devices delivers improved network performance and reliability, as well as reduces bottlenecks.

By utilizing ARK technology, the IoT industry can benefit from a more secure, robust and resilient network architecture- one that doesn't fall victim to data collusion, network tampering or single points of failure, delivering significant cost savings and efficiency gains.

Government. Governments and public sector entities around the world have been experimenting with blockchain technology over the past few years. This testing is now turning into adoption in many instances as the value of blockchain-powered infrastructure and public services is emerging. By utilizing blockchain technology, government operations can become more efficient and streamlined leading to more effective delivery of public services. Additionally, blockchain technology enables more streamlined internal processes which can lead to widespread cost savings.

Decentralized blockchain infrastructure removes single points of failure and provides additional layers of security and protection of critical government systems and citizen data. With blockchain allowing secure access to citizen records and data, trust is improved through radical transparency and accuracy enhancements. Fraud is deterred and compliance is upheld at all times due to the immutable and decentralized characteristics of blockchain.

Specific blockchain use-cases in government environments include digital identity, voting, payments, registries and record management. By transforming the way that governments are able to generate, process and share data, citizens are empowered via blockchain powered services.

By utilizing ARK blockchain technology, the government sector can benefit from operational efficiencies and streamlined processes, cost savings and disintermediation, increased trust and transparency along with improvements to both infrastructure and data security.

Supply Chain Management. Decentralized digital ledgers are allowing the supply chain management industry to get real-time oversight of player activity in their global supply chain network. The industry's key challenges of limited visibility and inaccuracies across its network create uncertainty. Lags and black holes can seemingly place inventory in multiple places at once, or more worryingly, nowhere at all. This poses a critical problem for a fast-paced industry that relies on getting the right product to the right place, at the right time.

This uncertainty, ultimately caused by gaps between departments and across business entities are a thing of the past with a complete blockchain solution. At its core, a blockchain is a ledger based on consensus. A consensus-based approach would mean that all nodes would agree about where inventory is at any one time.

Moreover, decentralized logic and workflows allow actions to be executed based on predefined conditions. This eliminates the 'middle-man' whether that be intermediary systems or labor, generating significant cost savings for supply chain organizations.

ARK technology can offer the supply chain industry greater oversight and control of inventory, enhanced data security, and automated processes, enabling increased efficiency and significant cost reduction.

11.7 Outreach

The ARK business entity does not intend to simply build. However, ARK also does not wish to participate in the empty hype train the crypto and blockchain industry appears to revere. In light of this, the ARK business entity executes and will continue to expand outreach initiatives that fulfill multiple tangible purposes, spreading awareness and adding strategic value to the overall ecosystem. The outreach initiatives ARK is focusing on includes the following:

Conferences. To date, ARK has sponsored nearly a dozen blockchain conferences and expos. The ARK business entity will continue to do this so long as these events continue to provide appropriate value in exchange for sponsorship and attendance. Conferences are useful to present ARK achievements and progress to the greater blockchain community. They also attract talent in the space to use ARK technology and allow peer review and feedback to take place. In addition, conferences position ARK in front of organizations and enterprises looking to utilize blockchain technology.

Hackathons. With blockchains containing the potential to impact the world as largely as the Web itself, it is logical to expose budding talent to ARK through universities and campuses around the world. Thus, ARK has sponsored nearly a dozen *hackathons*, which are short competitions among teams of computer science students and developers who create projects that are judged with prizes. ARK is utilizing a strategic partnership with Major League Hacking to create an ARK blockchain workshop, and also intends to enter the realm of virtual hackathons, where teams need not be in the same geographical location to compete.

Meetups and ARK Ambassador Program. Building a strong community is important to the success of any ecosystem. As such, agents of the ARK business entity attend meetups to give presentations on ARK technology and how people can get involved within the ecosystem. As blockchains gain in popularity, the frequency and size of these meetups around the world will increase and prominent ARK agents will not be able to keep up. The ARK Ambassador program will appear in 2019, where ARK agents train

and empower ARK enthusiasts to give these presentations and even host ARK-specific meetups of their own. After a certification, ARK Ambassadors can receive ARK bounties for representing the ARK business entity and ARK Ecosystem in the real world.

Market Research. The ARK business entity has recently acquired market research experts to identify the struggles within industries of interest and propose ARK-based solutions for them. This market research is paramount in reaching out to organizations and enterprises within these industries and start laying out how ARK technology can help them. As these organizations and entities use ARK technology more and more, their respective communities can merge with the ARK community, increasing its size and bringing more strategic value to the overall ecosystem.

Strategic Partnerships. There is a saying within the ARK community that ARK has 'no competitors, only future partners.' ARK partners with businesses, organizations, and other projects whenever tangible strategic value exists. This includes blockchain projects, exchanges, service providers, and others. Strategic partnerships allow the ARK business entity to gain access and capabilities in exchange for fulfilling a need for the partnering party, while operating funds remain protected. This also expands ARK's exposure.

Delegate Collaboration. The ARK business entity is fully aware of a large source of support and potential right next door, in the delegates of the ARK Public Network. Thus, the ARK business entity has no problem collaborating with mainnet delegates on initiatives that increase ARK exposure or bring strategic value to the ecosystem. Delegates launch campaigns to attract votes which usually include plans to deploy additional community services beyond securing the network. The ARK business entity has the ability to pour gasoline on these services in the form of additional seed funding beyond the block rewards that delegates receive. This can quickly add community impact to a delegate's deployed service. The ARK business entity also has the ability to include delegates in developing and deploying specific ARK products and

tools that have a key focus on expanding the overall ARK community.

Bounties & Contests. The ARK business entity is not solely responsible for deliverables by any means. In fact, the ARK Core and peripherals are on Github, where community developers help enhance the code. The *ARK Development & Security Bounty Program* awards community developers with ARK for helping. ARK is also partnered with Bugcrowd and launched a public bug bounty program with rewards for discovering vulnerabilities. ARK also ran documentation bounties for contributing to the ARK documentation repositories. ARK has also been known to run various contests for non-technical ARK community members. Those contest types are expected to continue and grow in 2019. ARK delegates and community members are welcome to collaborate with the ARK business entity via prize sponsorships.

Social & Rich Media. ARK has a strong presence on Steemit, LinkedIn, Slack, Discord, Reddit, Bitcoin Talk, Twitter, and Instagram. The ARK business entity also has a detailed blog on Medium that acts as a hub for public relations. ARK has useful videos on Youtube, and has specific plans to expand its Youtube presence throughout 2019. The ARK business entity also collaborates with delegates to increase the rich media available on its Youtube channel. ARK hosts a weekly audio podcast as well, available on iTunes, Google Play, Stitcher, Soundcloud, Spotify, and Castbox.

🔺 12 Conclusion

12.1 Blockchains are Here to Stay

Satoshi Nakamoto opened Pandora's box with Bitcoin. Blockchain technology has caused a new renaissance of inspiration that is growing worldwide. The potential for the technology is massive, and among the now thousands of blockchain projects in the space, working products and fulfilled promises are beginning to take shape. When inspiration hits a developer or organization, they will see that ARK has positioned itself to be the easiest path to success for them. Some of the largest tech companies in the world started with one person, on one computer, in one bedroom. ARK technology empowers this person to get ninety percent of the way there with a few clicks.

12.2 What the Future Holds for ARK

A successful ARK Ecosystem means that hundreds, if not thousands, of communities, businesses, enterprises, and organizations are using ARK technology to deploy blockchains custom tailored to their needs. Other blockchain projects with tokens on a restrictive mainnet begin to break off and form their own ARK-based network, addressing their **scalability** concerns and reaching higher planes of flexibility using ARK Logic. They experience the freedom of expression through the **sovereignty** they receive with ARK. They benefit from the **speed** and **security** ARK offers. They appreciate the **simplicity** of ARK technology. They receive much needed **support** from the ARK Public Network, ARK business entity, and ARK community. These ARK-based chains interoperate via SmartBridge Technology with a thriving ARK mainnet, bringing a true sense of unification without monopolization.

12.3 Get Involved

You play a key role in the success of ARK and you can bring tangible value that is truly appreciated by the whole of the ecosystem. If you like developing, you can improve the code on Github by tackling issues and submitting pull requests. You can apply your own ideas to develop additional peripherals and plugins using ARK. You can become an ARK mainnet delegate, or even launch your own chain.

If you aren't technically inclined, you can bring your own skills and talents to the table by asking questions, voting for delegates you support, accepting ARK for your business, receiving funding for an idea through the ARK Community Fund, and even helping the team in non-coding projects on the ARK Community Committee. ARK is for everyone, and together we can bring to the world the true vision of *Point. Click. Blockchain.*

▲ 13 Resources

Network Resources

wallet.ark.io: Download the official desktop wallet

android.ark.io: Download the official mobile wallet for Android

ios.ark.io: Download the official mobile wallet for iOS

explorer.ark.io: ARK Public Network blockchain explorer

Developer Resources

github.ark.io: Access the ARK codebase repositories

docs.ark.io: Technical documentation and guides

bounty.ark.io: ARK Development & Security Bounties

guidelines.ark.io: Protocols for contributors

Public Relations Resources

roadmap.ark.io: Progress on project statuses

blog.ark.io: Information on news and releases

steemit.ark.io: ARK Blog syndication on Steemit

Discussion Resources

slack.ark.io: Real-time ARK discussions and help

discord.ark.io: Real-time ARK discussions and help

reddit.ark.io: Official community Subreddit

bitcointalk.ark.io: ARK Bitcoin Talk forum page

Social & Rich Media Resources

twitter.ark.io: ARK Twitter account

instagram.ark.io: ARK Instagram account

youtube.ark.io: ARK Youtube channel

podcast.ark.io: ARK Crypto Podcast

Community Resources Not Affiliated with ARK.io

ArkDirectory.com: Community-managed library of links

ArkDelegates.io: Browse ARK Public Network delegates

ArkTippr.com: Interact with Reddit using ARK

ArkThoughts.com: Community opinions on ARK

ArkTimeline.com: Interactive timeline of ARK achievements

[46] http://www.assemblee-nationale.fr/15/pdf/rap-info/i1624.pdf
[47] http://www.assemblee-nationale.fr/15/pdf/rap-info/i1501.pdf
[48] https://blog.ark.io/what-is-the-ark-smartbridge-and-how-does-it-work-1dd7fb1e17a0
[49] https://codex.wordpress.org/Plugin_API
[50] https://vuejs.org/v2/guide/instance.html#Instance-Lifecycle-Hooks
[51] https://reactjs.org/docs/state-and-lifecycle.html
[52] https://en.wikipedia.org/wiki/Publish%E2%80%93subscribe_pattern
[53] https://blog.ark.io/making-cross-chain-smart-contracts-on-ark-via-hyperledger-fabric-e69149b1e12c
[54] https://arkaces.com
[55] https://bitcoinfees.info/
[56] https://www.investopedia.com/terms/f/fiatmoney.asp
[57] https://lisk.io/documentation/lisk-protocol/consensus
[58] https://www.researchgate.net/publication/228913406_A_Study_on_Test_Coverage_in_Software_Testing
[59] https://github.com/ArkEcosystem/AIPs/blob/master/AIPS/aip-11.md