

ARCBLOCK™
TECHNICAL WHITE PAPER

CRYP2NOVA

The world's first blockchain ecosystem for
building and deploying decentralized applications.

VERSION 1.1.2 (12/25/2017)

COPYRIGHT © 2017 ARCBLOCK FOUNDATION LIMITED. ALL RIGHTS RESERVED.

Archived copy · cryp2nova.com

NOTICE

NOTHING IN THIS TECHNICAL WHITEPAPER CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISER BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER ARCBLOCK FOUNDATION LTD. (THE FOUNDATION), ANY OF THE PROJECT TEAM MEMBERS WHO HAVE WORKED ON THE ARCBLOCK PLATFORM (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE ARCBLOCK PLATFORM IN ANY WAY WHATSOEVER (THE ARCBLOCK TEAM) NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS TECHNICAL WHITEPAPER, THE BUSINESS WHITEPAPER, THE WEBSITE AT HTTPS://WWW.ARCBLOCK.IO/ OR ANY OTHER MATERIALS PUBLISHED BY THE FOUNDATION.

All contributions will be applied towards the Foundation's objects, including without limitation promoting the research, design and development of, and advocacy for a scalable, extensible, cost efficient, protocol-agnostic and easy-to-use platform for building and deploying decentralised blockchain applications, which would overcome many of the existing technological barriers faced by existing blockchains, and which is designed to be a self-evolving ecosystem.

This Technical Whitepaper is intended for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein below may not be exhaustive and does not imply any elements of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where this Technical Whitepaper includes information that has been obtained from third party sources, the Foundation and/or the ArcBlock team have not independently verified the accuracy or completion of such information.

This Technical Whitepaper does not constitute any offer by the Foundation or the ArcBlock team to sell any ABT (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in this Technical Whitepaper is or may be relied upon as a promise, representation or undertaking as to the future performance of the ArcBlock Platform. The agreement between the Foundation (or its affiliate) and you, in relation to any sale and purchase of ABT is to be governed by only the separate terms and conditions of such agreement.

By accessing this Technical Whitepaper or any part thereof, you represent and warrant to the Foundation, its affiliates and the ArcBlock team as follows:

(a) you acknowledge, understand and agree that ABT may have no value, there is no guarantee or representation of value or liquidity for ABT, and ABT is not for speculative investment;

(b) none of the Foundation, its affiliates, and/or the ArcBlock team members shall be responsible for or liable for the value of ABT, the transferability and/or liquidity of ABT and/or the availability of any market for ABT through third parties or otherwise;

(c) in any decision to purchase any ABT, you have not relied on any statement set out in this Technical Whitepaper;

(d) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be); and

(e) you acknowledge, understand and agree that you are not eligible to purchase any ABT if you are a citizen,

Archived copy · cryp2nova.com

national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of ABT would be construed as the sale of a security (howsoever named) or investment product and/or (ii) in which access to or participation in the ABT token sale or the ArcBlock Platform is prohibited by applicable law, decree, regulation, treaty, or administrative act, and/or (including without limitation The United States of America, The People's Republic of China, New Zealand, and the Republic of Korea).

The Foundation and the ArcBlock team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person. Prospective purchasers of ABT should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the ABT token sale, the Foundation and the ArcBlock team.

The information set out in this Technical Whitepaper is for community discussion only and is not legally binding. The agreement for sale and purchase of ABT shall be governed by a separate Token Sale Terms and Conditions setting out the terms and conditions of such agreement (the Token Sale Terms and Conditions), which shall be separately provided to you or made available at https://www.arcblock.io/. In the event of any inconsistencies between the Token Sale Terms and Conditions and this Technical Whitepaper, the Token Sale Terms and Conditions shall prevail.

All statements contained in this Technical Whitepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation and/or the ArcBlock team may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements. These forward-looking statements are applicable only as of the date of this Technical Whitepaper and the Foundation and the ArcBlock team expressly disclaims any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

This Technical Whitepaper may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of this Technical Whitepaper, the English language version shall prevail. You acknowledge that you have read and understood the English language version of this Technical Whitepaper.

No part of this Technical Whitepaper is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Foundation.

CRYP2NOVA

Archived copy · cryp2nova.com

INTRODUCTION

PURPOSE

The purpose of this document is to provide a high-level technical overview of the ArcBlock platform. It assumes that the reader has a basic understanding of cloud computing, decentralized applications, and blockchain technology. A list of resources is provided for those who would like to develop a foundational understanding of blockchain technology.

SCOPE

This document provides a technical overview of ArcBlock, a blockchain ecosystem for building and deploying decentralized applications. It describes core elements of the service and provides details about the architectural design of critical components.

The information in this document is intended for informational purposes only. ArcBlock may make improvements or changes to the products, architectural design, or programs described in this document at any time without notice.

RELATED DOCUMENTS

ArcBlock Official Website: https://arcblock.io

CRYP2NOVA

Archived copy · cryp2nova.com

TABLE OF CONTENTS

Introduction 2
- Purpose 2
- Scope 2
- Related Documents 2

Overview 5
- Problems with Today's Blockchains 5
  - Poor Performance 5
  - Not Consumer Friendly 5
  - Cost 6
  - Platform Lock-In 6
  - Lack of Features 6
- The ArcBlock Platform 7
- ArcBlock's Advantages 8
  - Built for the New Token Economy 8
  - Optimized for the Best Experience 8
  - Built for the Cloud 8
  - Built with an Open Standard 9

Architecture 9
- Design Principles 9
- System Architecture 9
  - Open Chain Access Protocol 10
  - Blocklet 10
  - Blocklet Components 11
  - Decentralized Pub/Sub Gateway 11
  - Marketplace and Token Economy 11
- Cloud Nodes 11

Core Components 12
- Open Chain Access Protocol 12
  - Open Chain Access Layer 12
  - Chain Adapters 13
  - Chain Adapters Marketplace 13

CRYP2NOVA

Archived copy · cryp2nova.com

Relationship with Blockchain as a Service 14
Design Principles and Inspiration 14
Blocklet 14
Microservice Architecture 15
Serverless Computing 15
Blocklet Types 15
Off-Chain Logic 15
Off-Chain and On-Chain Logic 16
Asset and Resource Handling 16
Smart Contracts 16
Oracle 16
Blocklet Implementation 16
Blocklet Components 17
Decentralized Pub/Sub API Gateway 17
API Gateway 17
Pub/Sub 18
Decentralized and Secured 18
Decentralized Media and Assets 18
Client Library/Framework 19
Algorand 20
The Token Economy and the Service 21
The ArcBlock Token (ABT) 21
The Miners 22
Resource Miners 22
Component Miners 22
The ArcBlock Marketplace 22
Token Foundation Services 22
Application Tokens 23
Future Work 23
Acknowledgements 23

Archived copy · cryp2nova.com

OVERVIEW

ArcBlock is a platform and an ecosystem for building and deploying decentralized blockchain applications. The platform goes beyond providing the necessary foundational components for using blockchain to power complex business rules. It connects your existing system to blockchain networks, enabling you to automate business processes using the data and identities associated with existing systems.

ArcBlock's primary goal is to remove the barriers that have slowed blockchain adoption among the general public. We're also passionate about developing unique approaches that will significantly advance blockchain development.

PROBLEMS WITH TODAY'S BLOCKCHAINS

Blockchain technology is still in its infancy. There are many issues preventing developers and businesses from creating widespread, decentralized blockchain applications.

POOR PERFORMANCE

Performance is one of the main challenges facing current blockchain technology. The blockchain that Bitcoin uses is designed to handle seven transactions per second, and Ethereum can only handle a few more. As of December 2017, a simple CryptoKitties[1] application can slow Ethereum and increase transaction fees dramatically.

Today's consumer applications must be able to handle tens of millions of active users on a daily basis. In addition, some applications will only become meaningful when critical mass is reached. The platform itself must be able to handle a large number of concurrent users.

A good user experience demands reliable feedback with only sub second delays. Longer delays frustrate users and make applications built on a blockchain less competitive with existing non-blockchain alternatives.

NOT CONSUMER FRIENDLY

Today's blockchain applications are built for the few tech whizzes who know how to use them, rather than mainstream consumers. Nearly all blockchain applications require users to either run a blockchain node or install a "light node." The learning curve and effort involved has delayed adoption among the general public.

For example, while the Ethereum-based game CryptoKitties is probably the most user-friendly decentralized app ever built, it still requires the user to install the Metamask light wallet[2] browser extension. Users also need to know how to buy ethers securely and use them with Metamask.

To attract large numbers of people, blockchain applications need to be as simple as today's web and mobile apps. Blockchain technology should be completely transparent to the consumer.

---

1 CryptoKitties craze slows down transactions on Ethereum (http://www.bbc.com/news/technology-42237162)
2 Metamask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum dApps right in your browser without running a full Ethereum node. (https://metamask.io/)

Archived copy · cryp2nova.com

COST

The extremely high cost of using blockchain technology is a major barrier to mainstream adoption. It also limits developers who need the flexibility to build free services. Just like today's web and mobile apps, users shouldn't have to pay for every minor action. Similar to the Internet, blockchain technology should be able to support free applications.

Making blockchain free to use is key to widespread adoption. A free platform will also empower developers and businesses to create valuable new services they can monetize, rather than having users pay fees to use the blockchain network.

PLATFORM LOCK-IN

As with the early days of any computing technology, blockchains have critical "platform lock-in" problems. Developers have to decide which blockchain to support, then implement platform-specific code that makes it very difficult to switch an application to a different blockchain later on.

Developers don't want to be locked into working with a certain blockchain technology. They need the freedom to evaluate, use, and switch between options. Some applications may even need to run on multiple platforms to provide the best user experience.

LACK OF FEATURES

People have high expectations for blockchain—the news media, evangelists, and journalists paint a bright future for decentralized applications for the public, especially with the increasingly high prices of cryptocurrencies. In reality, however, blockchain technology is still in its infancy. Most blockchain services lack rich features and don't have a mechanism to encourage the community to contribute to the feature stacks.

Blockchain protocols make them very easy to fork, and there's been a recent spike in forks created for various purposes. Unfortunately, forks typically only improve on the forked branch, splitting the community and computing resources. The incentive mechanisms for blockchains just aren't designed to encourage contributions to the blockchain tech stack yet.

THE ARCBLOCK PLATFORM

ArcBlock solves these problems through its revolutionary new design. Unlike its predecessors, ArcBlock is a **platform service**, rather than a standalone software package or set of APIs. ArcBlock is a comprehensive solution that combines blockchain technology with Cloud Computing.

ArcBlock is an **incentive-driven marketplace** for reusable services, components, and even applications. "Miners" in ArcBlock platform not only bring computing resources, more over they help to build the platform together by providing reusable components, new services, and even ready to deploy applications. People who contributed resources or services will be rewarded with tokens to form a positive, self-growing platform that continues to evolve on its own. The ArcBlock platform service isn't our creation alone. It's developed by the entire ArcBlock community—we're just kick-starting a new blockchain revolution.

ArcBlock's introduction of the **Open Chain Access Protocol** enabled open connectivity over multiple blockchain protocols. Developers now have the freedom to evaluate blockchain protocols, and even

Archived copy · cryp2nova.com

switch back and forth between them. The Open Chain Access Protocol makes it easy to implement new blockchains as the technology evolves. It eliminates the platform lock-in issue and enables applications to run on multiple blockchain fabrics, vastly improving the developer and user experiences.

Blocklet is another revolutionary component that takes advantage of the latest microservice architecture and serverless computing technology. Blocklet is a high-level application protocol that can be implemented with any platform or language. It leverages the full capacity of the native platform and offers the same level of performance, rather than running on a low-performing virtual machine.

Blocklet does more than access blockchains. It connects to any existing data source, and performs both on-chain and off-chain computing.

Our unique design aims to provide a high-performance, user-friendly, cost efficient, and protocol-agnostic platform. We believe that ArcBlock represents a major technological advance that will usher in the 3.0 generation of blockchain applications.

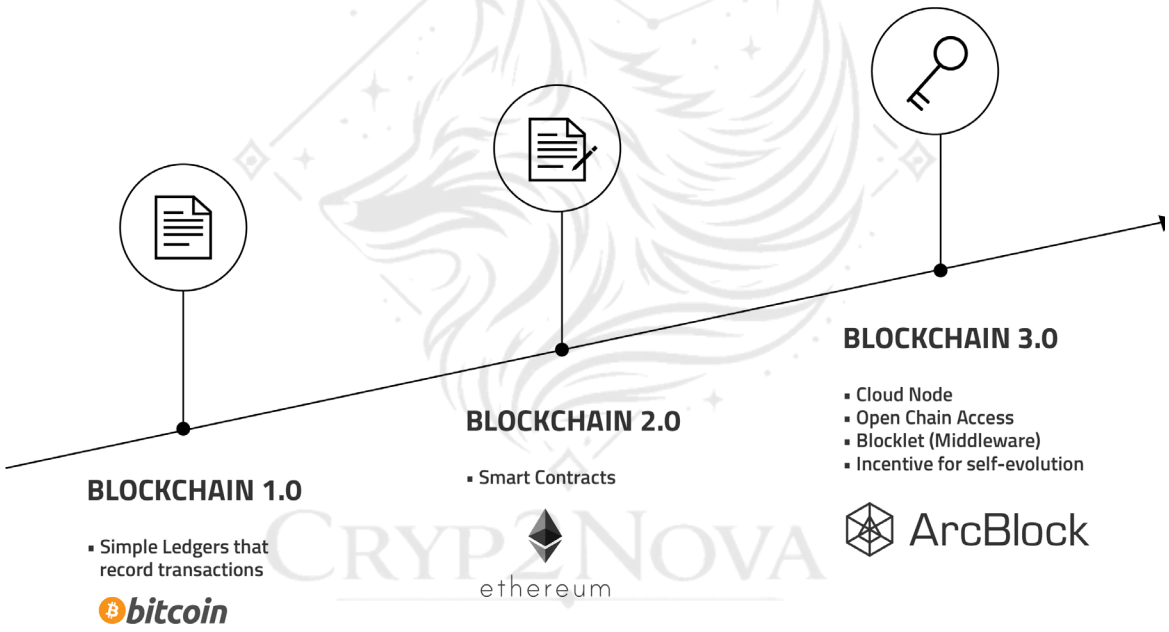


Fig: Road map toward Blockchain 3.0

ARCBLOCK'S ADVANTAGES

In addition to solving the common problems outlined above, building and deploying decentralized blockchain applications with ArcBlock has significant advantages over the vendor-specific frameworks available in today's market.

BUILT FOR THE NEW TOKEN ECONOMY

ArcBlock is a self-evolving ecosystem—not just a software platform built by one centralized

Archived copy · cryp2nova.com

organization. We at ArcBlock Foundation Limited and the ArcBlock Foundation are only jump starting the project; the platform will continue to develop and grow on its own.

The entire ArcBlock service is driven by the token economy. Rather than a basic service platform, ArcBlock is an economy driven by incentives that encourage the blockchain community to work together to build a better ecosystem.

OPTIMIZED FOR THE BEST EXPERIENCE

We built the ArcBlock platform using a "top-down" strategy that centers on the user experience. In contrast, many existing solutions focus on the blockchain technology itself at the expense of user friendliness. Applications built with ArcBlock offer reactive, real-time experiences. Users can simply access them from a web browser (no additional plugins required), or download a mobile app directly from an app store. Either way, the process is familiar.

ArcBlock also dramatically improves the developer experience. There's no need to deal with low-level blockchain protocols. With our mock blockchain adapters, engineers don't even have to run local blockchain test nodes to start developing and testing their applications.

BUILT FOR THE CLOUD

ArcBlock is designed to run natively in the cloud. It can also run on a single computer for testing and development.

This design principle makes ArcBlock fundamentally different from many other platforms in the blockchain world. In ArcBlock, a node can be a "logical computer" comprised of one or more virtual machines, or a group of cloud services working together as a computing environment. This approach marks a significant step forward that will help elevate blockchain and decentralized applications to the next level, including our patent pending technologies.

ArcBlock will initially build on top of AWS and Windows Azure, then expand to support Google Compute Engine, major cloud computing players in China, and other platforms.

BUILT WITH AN OPEN STANDARD

ArcBlock is built with an open standard. We're trying our best not to reinvent the wheel and to build for the application developer's wants and needs. In addition to open sourcing our core components, we will also actively contribute to a variety of blockchain technology communities.

Our team members are actively involved with a range of standards organizations, non-profit foundations, and committees. These currently include the W3C Blockchain Community Group Community Group, IEEE Standard Association's Blockchain Community, Enterprise Ethereum Alliance, Linux Foundation, and Hyperledger Foundation. This list will expand over time.

Archived copy · cryp2nova.com

ARCHITECTURE

ArcBlock aims to build a **scalable**, **extensible,** and **easy-to-use** platform for building and deploying decentralized blockchain applications.

DESIGN PRINCIPLES

ArcBlock's design is based on following core principles:

- The user experience comes first.
- Performance matters.
- The system will be built on an open standard.
- The system will build upon an Incentive-driven economy.

SYSTEM ARCHITECTURE

The ArcBlock platform introduces a suite of revolutionary technologies designed to mainstream blockchain applications by making them easy for the average consumer to use.

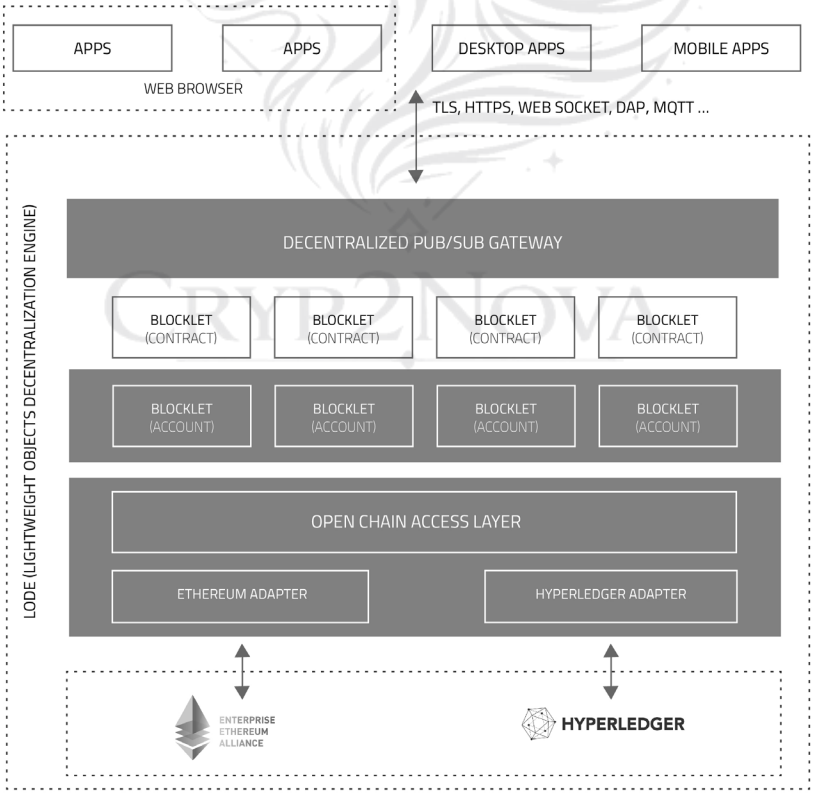


Fig: High-level Overview of ArcBlock

Archived copy · cryp2nova.com

OPEN CHAIN ACCESS PROTOCOL

Our open source protocol provides an abstract layer for accessing underlying blockchains. Similar to an ODBC or JDBC interface to a set of databases, our Open Chain Access Protocol enables your application to work on different blockchains. There's no need to alter your business logic or work with multiple chain technologies.

Chain Adapters can be built by the community and encouraged by the incentive mechanism. This will enable ArcBlock to support many blockchain protocols and continue to improve.

BLOCKLET

Blocklet is a serverless computing architecture component for running various types of applications. Use Blocklet for smart contracts, oracle, resource and asset handling, and off-chain business logic. Blocklet communicates with blockchains through ArcBlock's Open Chain Access Protocol, and can be orchestrated with our Algorand-based consensus algorithm.

Anyone can use Blocklet to build services and components and contribute them under the incentive system. Community members will receive tokens when others use their contributions.

BLOCKLET COMPONENTS

Blocklet Components are pre-built blocklets that form the foundation of the ArcBlock platform. Most of ArcBlock's features (such as its token services, user identity services, etc.) are implemented with them. Blocklet Components are highly reusable and customizable.

Incorporate our pre-built Blocklet Components into your applications to get up and running fast. We provide components for user identity management, utility tokens, wallets, messaging, notification services, and more. Use them out-of-the-box, or as customizable starting points for your own creations.

Blocklet Components can also be built and contributed by the community. They are managed through the ArcBlock Marketplace app.

CRYP2NOVA

DECENTRALIZED PUB/SUB GATEWAY

A distributed messaging system supports pub/sub and acts as an API gateway for Blocklets. ArcBlock's gateway uses a decentralized design and secure communication channels. Your applications will run in both web browsers and mobile apps, giving users reactive, real-time experiences.

The gateway supports various network protocols by default, including WebSocket, DDP, HTTPS, and MQTT. Advanced developers can extend the gateway with new network protocols to fit their needs.

MARKETPLACE AND TOKEN ECONOMY

ArcBlock comes with a fully customizable token economy manager for apps built on the platform. Applications can even build unique utility tokens that inherit all ArcBlock features.

The ArcBlock Marketplace is a native application built on ArcBlock to allow the community contribute and exchange reusable components (e.g. Chain Adapters, Blocklets, or even applications) .

Archived copy · cryp2nova.com

The diagram below shows a high-level view of the platform architecture. Detailed descriptions of some of the core components appear in the next section.

CLOUD NODES

While using a group of cloud services as a node may seem like an unusual approach, a physical computer is simply a group of hardware components that work together (CPU, memory, external storage, bus, network interfaces) in one box. Aside from how the components are distributed and communicate with each other, they're essentially the same. ArcBlock is the first blockchain platform to treat cloud services as nodes, achieving a much higher level of abstraction, enhanced performance, and even better security. We believe this approach will likely become the de facto standard for future blockchain platform design, and we as a pioneer will lead the trend as technology evolves.

Although ArcBlock's preferred node is a cloud node, you can still run ArcBlock in a single traditional node like a server box. In a test or private environment, developers likely run the node locally, or in their test server boxes.

Using a cloud node won't compromise the decentralization and security of the system. In fact, it takes decentralization and security to the next level.

The cloud platform's own security is enforced by cloud service providers. Most likely, the servers and services from a cloud service provider will be more secure and reliable than self-hosting servers, and far more secure and reliable than peer-to-peer connected nodes from homes or mining farms.

The decentralization aspect of using a cloud node is even more interesting, since a cloud node is likely a distributed service that runs on multiple servers from multiple availability zones, or even different regions. In the future, cloud nodes could be offered by various providers and cloud computing vendors. Some may even be self-hosted mining service providers. This makes the system much more decentralized indeed.

CRYP2NOVA

CORE COMPONENTS

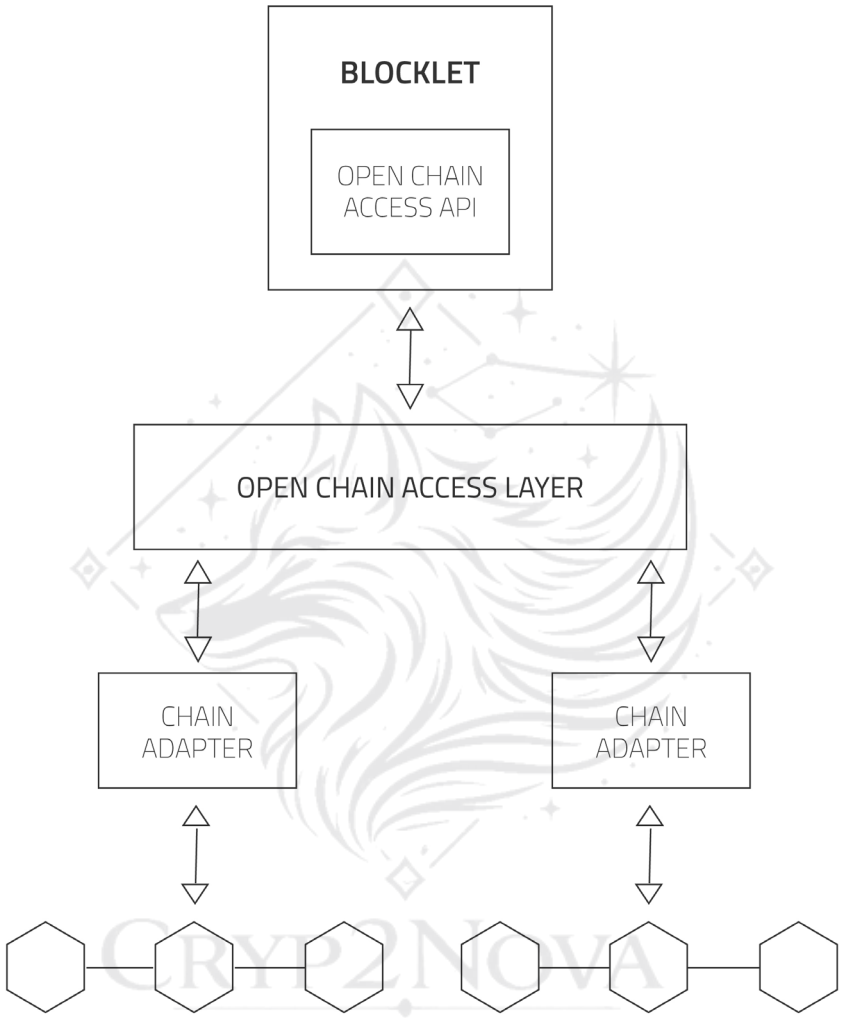
The following sections offer more detailed descriptions of our key components and core algorithm. This section assume that you have an advanced understanding of blockchain technology and computer science. If you're not interested in detailed information about the components and would rather learn more about using the platform, feel free to skip this section.

OPEN CHAIN ACCESS PROTOCOL

ArcBlock's Open Chain Access Protocol enables your application to adapt to a variety of blockchain protocols including Bitcoin, Ethereum, Hyperledger, and more. The Open Chain Access Protocol will be open sourced with an MIT license so that everyone in the blockchain community will be able to

Archived copy · cryp2nova.com

contribute, create extensions, and make improvements. We will develop the protocol in private mode, then open source it once we reach the release candidate milestone.



OPEN CHAIN ACCESS LAYER

The Open Chain Access Layer defines high-level, generic APIs that enable open connectivity and access to a range of blockchain protocols. The Layer is supported by a Chain Adapter under layer. Each Chain Adapter is implemented for a specific blockchain protocol.

Archived copy · cryp2nova.com

The Open Chain Access Layer has three levels of APIs:

Level	Description
Level 1: **Common Chain APIs**	This set of APIs provides the foundation for the Open Chain Access APIs. Any Chain Adapters must support all of the APIs included in this level.
Level 2: **Common Chain Data APIs**	This set of APIs enables fundamental access to blockchain data, and treats each blockchain under layer as a finite state machine. Chain Adapters may either support the APIs at this level, or alternate capabilities. The set includes APIs that allow applications to query the supported capabilities. A Chain Adapter must support all of the APIs included in this level. However, they may implement a different capacity set.
Level 3: Native Chain APIs	This advanced API set exposes the native features of underlying blockchain protocols. While supporting this set is optional, it will maximize your application's ability to use native blockchain features. Supporting the API set at this level is optional for Chain Adapters.

CHAIN ADAPTERS

ArcBlock's Open Chain Access Layer enables the platform to support multiple blockchain protocols. Application developers can choose from several different blockchains, node types, and deployment types. ArcBlock's Chain Adaptors are the implementations that make the Open Chain Access Layer possible.

Chain Adapters work like device drivers to translate blockchain under layer protocols into the unified APIs defined in the Open Chain Access Layer. Some of the Chain Adapter implementations require you to combine on-chain and off-chain implementation works together. The Chain Adapter is also assigned one of three categories, based on the Open Chain Access Layer API set it has implemented.

We plan to implement Chain Adapters for Bitcoin Blockchain, Ethereum, and Hyperledger first. After we open source the code, anyone will be able to contribute, improve the protocol, or implement their own code. We also plan to support additional blockchain protocols.

CHAIN ADAPTERS MARKETPLACE

Chain Adapters that have been developed or improved by the community will be made available in the ArcBlock marketplace so that everyone can use them. The people who contributed to the adapter will receive rewards when others use it. The incentive model will encourage the community to develop more and better Chain Adapters. In time, ArcBlock will be able to offer a line of high-performance, high-quality Chain Adapters for various blockchains.

Archived copy · cryp2nova.com

RELATIONSHIP WITH BLOCKCHAIN AS A SERVICE

In the past 12 months, several leading cloud platform providers began offering a new type of platform called Blockchain as a Service (BaaS). BaaS platforms typically offer users a permissioned or public chain, and they're usually optimized for a specific deployment or node type. IBM Cloud (aka Bluemix) BaaS[3], which offers a Hyperledger Fabric service, was one of the earliest providers. While Microsoft Windows Azure also offers a BaaS platform[4], it mainly targets the test environment and fast spin-up for developers. Amazon AWS hasn't officially offered a BaaS yet, but there are third-party VM images that help users quickly deploy blockchain nodes with AWS EC2 instances.

Existing BaaS platforms work perfectly with ArcBlock. While they simplify the process of deploying blockchain for users, ArcBlock simplifies the process of developing and deploying blockchain apps for software engineers. The first phase of ArcBlock's implementation will include integrating with cloud computing platforms (through the AWS SDK, for example), so that users can manage BaaS services from directly within ArcBlock applications.

DESIGN PRINCIPLES AND INSPIRATION

To design the Open Chain Access Protocol, we investigated many existing customer solutions, talked to real developers, and learned from the evolution of computers and database systems. For example, the structure for the Open Chain Access Layer was inspired by the open connectivity design seen in databases.

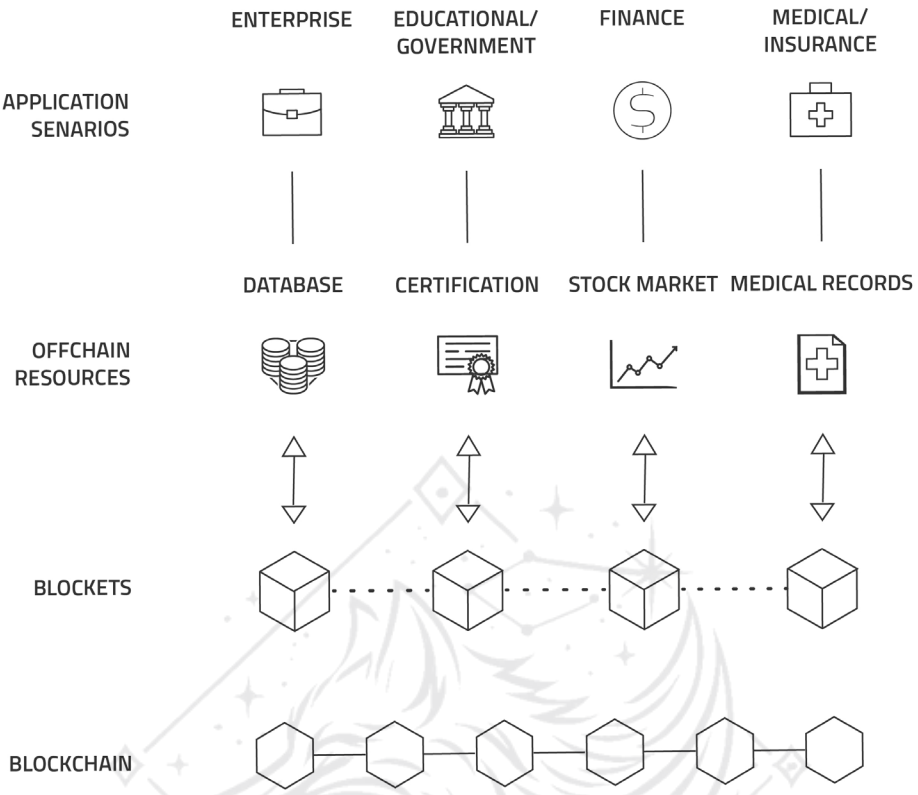
A look back at the development of database systems and applications reveals many similarities with the evolution of blockchain technology[5]. The position of the blockchain in a typical system is very much the same as the database in a database application system. In many scenarios, it's fair to say that a blockchain is actually acting as a distributed database. Most of the blockchain itself is built on top of a database, including Bitcoin and Ethereum. That said, we can find inspiration in how database systems evolved.

BLOCKLET

Blocklet is the core of ArcBlock. More than an application protocol, it's also a software architect that lays the foundational building blocks of ArcBlock itself. The ArcBlock platform is built on a series of Blocklets. The Open Chain Access Protocol allows Blocklet to communicate with under layer blockchains. The Distributed pub/sub gateway allows Blocklets to communicate with the client-side code live in the user's browser or mobiles apps. In short, Blocklets are at the center of the entire system.

3 IBM offers Blockchain as a Service https://www.theregister.co.uk/2017/03/20/blockchain_as_a_service_ibm/
4 Blockchain on Azure https://azure.microsoft.com/en-us/solutions/blockchain/
5 C. Mohan, Tutorial: Blockchains and Databases, 2016, VLDB Endowment, https://dl.acm.org/citation.cfm?id=3137830

Archived copy · cryp2nova.com



MICROSERVICE ARCHITECTURE

Microservice architecture[6] is a perfect match for blockchain applications. A variant of the service-oriented architecture (SOA) style, microservice architecture structures an application as a collection of loosely coupled services. The services should be fine-grained and the protocols lightweight. Deconstructing an application into a variety of smaller services improves modularity and makes the application easier to understand, develop, and test.

ArcBlock is designed as an event-driven microservice that uses Blocklet technology to overcome the inherent limitations of the blockchain. Blocklet communicates with the blockchain under layer through the Open Chain Access Protocol, allowing the application to access external data securely while also maintaining data integrity.

SERVERLESS COMPUTING

Serverless computing[7] is a cloud computing execution model in which the cloud provider dynamically manages the allocation of machine resources. Most serverless vendors offer compute runtimes or function as a service (FaaS)[8] platforms, which execute application logic but do not store data.

Serverless computing models also work well with blockchains. Most of the Blocklets can be implemented as a serverless program. Manage Blocklets through AWS Lambda, Windows Azure Functions, or another serverless execution environment.

6 Microservices https://en.wikipedia.org/wiki/Microservices
7 Serverless computing https://en.wikipedia.org/wiki/Serverless_computing
8 Function as a service (FaaS) https://en.wikipedia.org/wiki/Function_as_a_service

Archived copy · cryp2nova.com

Note that microservice architecture and serverless computing involve different levels of abstraction. Serverless computing can be used to implement a microservice that fits perfectly within a microservice architecture. However, developers can also use serverless computing for other purposes, and it's not always necessary to use serverless computing to implement microservices.

BLOCKLET TYPES

Blocklet is inherently flexible and can be used to develop various kinds of applications. This section describes some common types of blocklets. Bear in mind, however, that a Blocklet could consist of one or more of the following units of business logic packaged together.

Off-Chain Logic

Because Blocklet is a native microservice, it can access data sources other than the blockchain. For example, it can connect to a database, external restful API, or any other data source. Blocklet can be used to develop any application logic—even logic that's not related to blockchain. Using Blocklet for standard application development has no overhead.

Real-life, decentralized applications often run quite a few logical components off-chain. Blocklet provides a total solution for application development so that engineers won't need to use different frameworks to handle different parts of their applications.

Off-Chain and On-Chain Logic

It's very common for an application's business logic to need both on-chain and off-chain handling, and to require the respective data to be connected. For example, on-chain code can't access external data and events, such as time or market. Calling code or data outside of an on-chain smart contract or blockchain breaks the general trust barrier and reduces confidence in the authenticity of transactions. In these cases, an off-chain Blocklet acts as a bridge that connects on-chain and off-chain logic to bring the full business logic together.

Asset and Resource Handling

Applications usually need to handle resources and assets like photos, videos, music, and documents. Because blockchain isn't designed to handle large amounts of data, a typical blockchain application handles those resources and assets with off-chain solutions. While there are different ways to accomplish this, the traditional solution involves using a service like AWS S3, or a more decentralized solution like IPFS.

Regardless of the approach you take, Blocklet will be able to communicate with your assets and resource storage system. Sometimes assets may need to be mapped with their on-chain token or identifiers, or verified through the records on the blockchain. Blocklet is the perfect location for these kinds of logic.

Archived copy · cryp2nova.com

Smart Contracts

By communicating with on-chain code securely through the Open Chain Access Protocol, Blocklet enables you to implement high-performance smart contracts while maintaining the trust barrier and verifying the authenticity of transactions.

It's up to the engineer to decide how much logic should run on-chain vs. off-chain. At one extreme, the engineer could simply treat the blockchain as a state machine and put most of the business logic inside the Blocklet. At the other extreme, the engineer might develop a complex, fully on-chain contract where the Blocklet merely serves as a stub for triggering or monitoring activity from the on-chain execution.

Oracle

In Blocklet design, Oracle is simply a type of smart contract that takes external data sources as event triggers. Blocklet makes it easy to implement Oracle by design.

Blocklet-based design also compels engineers to consider the division between on-chain and off-chain logic during the design and development phases. This improves the efficiency of these phases without compromising security and trust.

BLOCKLET IMPLEMENTATION

In the first phase of ArcBlock development, we will implement Blocklets with a local test environment and AWS. The local implementation is for test purposes only. Production will be based on AWS so that we can take advantage of the many advanced design features AWS offers.

In the future, we will support Windows Azure, Google Compute Engine, IBM Bluemix, and other computing platforms. We also plan to support Docker and open source FasS solutions for Blocklet so that users can easily build and deploy their own Blocklets without using any cloud services.

Because Blocklet itself is a type of application protocol and architecture, it's possible to implement it with different languages and frameworks. Our initial implementation will be based on Node.js and GO.

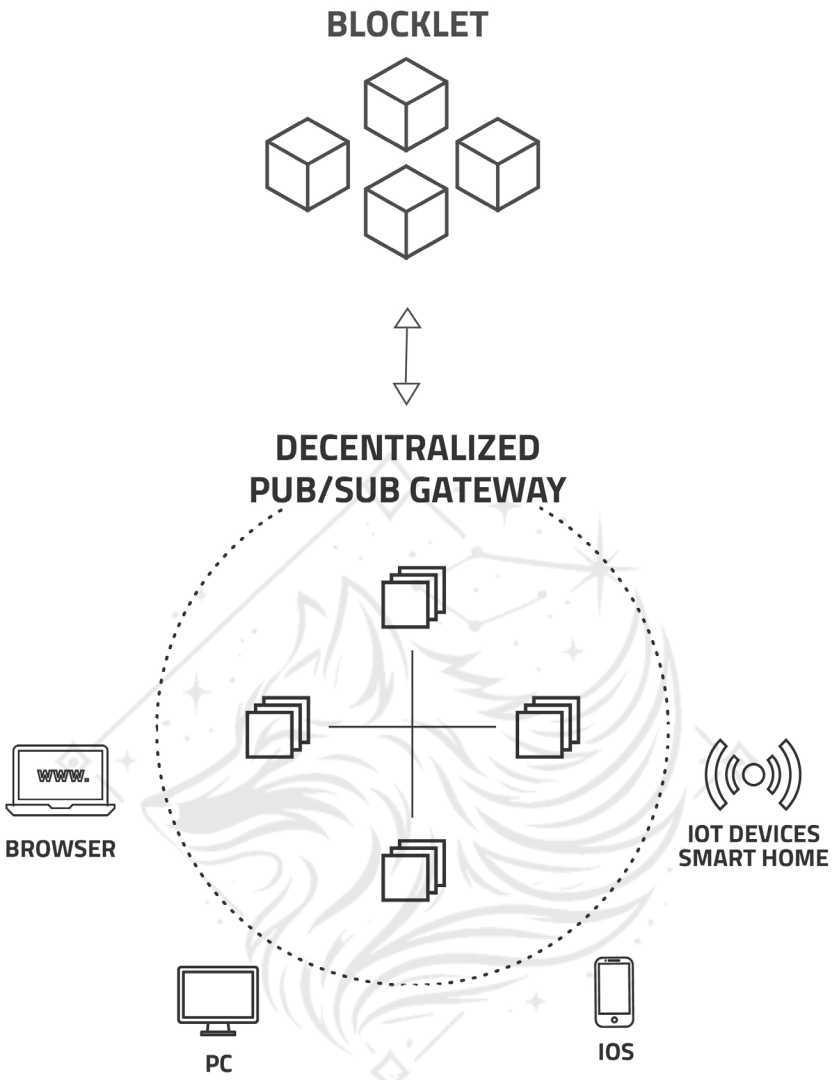
BLOCKLET COMPONENTS

Blocklet Building Blocks are pre-built blocklets that lay the foundation for the ArcBlock platform and most of its features, such as token and user identity services. Blocklet Building Blocks are highly reusable and customizable components.

DECENTRALIZED PUB/SUB API GATEWAY

A distributed messaging system supports pub/sub and acts as an API gateway for Blocklets. ArcBlock's gateway uses a decentralized design and secure communication channels. Your applications will run in both web browsers and mobile apps, giving users reactive, real-time experiences.

Archived copy · cryp2nova.com



API GATEWAY

An API gateway is essential in microservice architecture. An API gateway is a façade that provides a simple API interface to a complex subsystem. It essentially decouples the interface that clients see (in our case API consumers, which could be mobile apps, web clients, or thin clients) from the underlying implementations. In ArcBlock, all features are implemented with Blocklets. Rather than communicating directly with clients, Blocklets communicate through the API Gateway.

The gateway supports various network protocols by default, including WebSocket, DDP, HTTPS, and MQTT. Advanced developers can extend the gateway with new network protocols to fit their needs.

Archived copy · cryp2nova.com

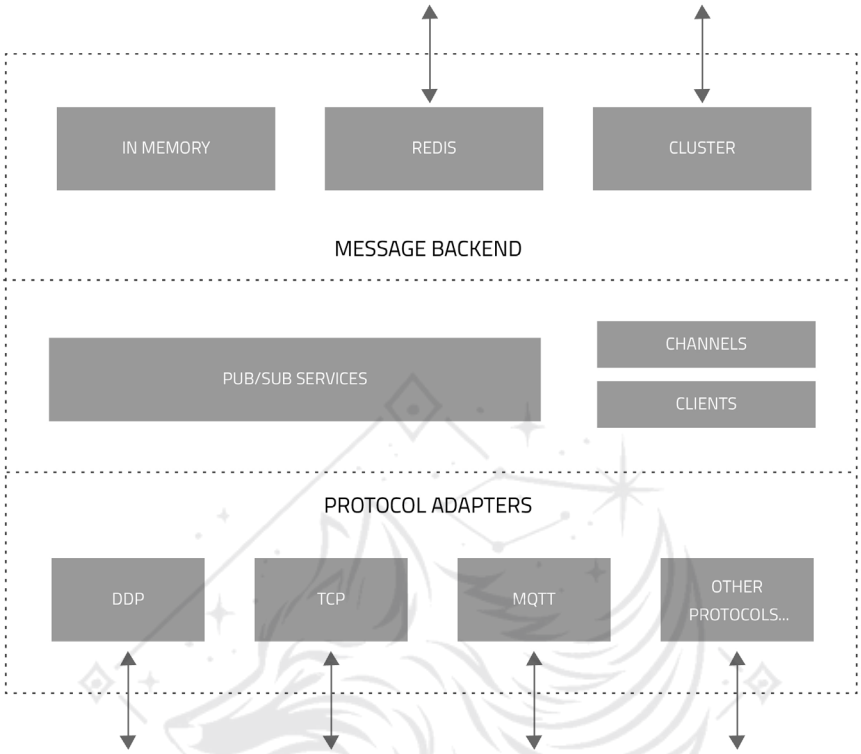


Fig: A Simple Reference Implementation in Node.js (as of Dec 2017)

PUB/SUB

Publish–subscribe is a messaging pattern where message senders (publishers) categorize published messages into classes without knowing which subscribers will receive them, if any. Similarly, subscribers only receive messages assigned to the classes they've expressed interest in, without knowing which publishers there are, if any.

The publish–subscribe pattern is a sibling of the message queue paradigm. It's typically a single piece in a larger message-oriented middleware system. Most messaging systems support both the pub/sub and message queue models in their APIs. This pattern provides greater network scalability and a more dynamic network topology, resulting in decreased flexibility in terms of modifying the publisher and the structure of the published data (This is not a disadvantage for blockchain applications).

DECENTRALIZED AND SECURED

We use a completely decentralized design to implement and simplify cloud services. ArcBlock's API Gateway can be used out-of-the-box with zero configuration—just start it up and it will do its magic. It also features name-based addressing, clusters (i.e. automatic load balancing), and perfect secrecy (all network traffic is encrypted).

Archived copy · cryp2nova.com

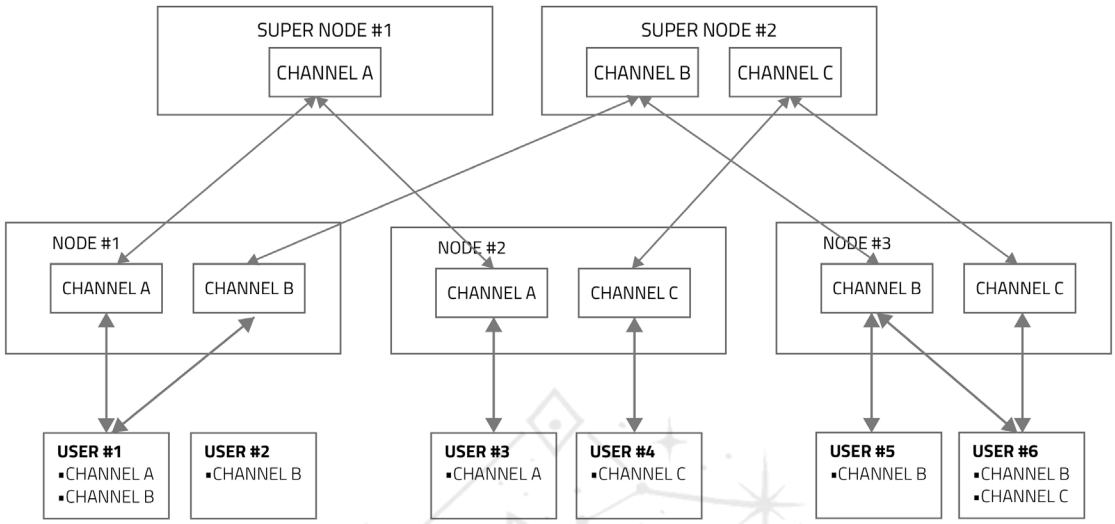


Fig: How decentralized messaging and pub/sub works

DECENTRALIZED MEDIA AND ASSETS

While ArcBlock's core components weren't designed to handle media and assets, Blocklet can be used to handle them with support from other systems. Blocklet can also help you create off-chain data, or verify off-chain data with the on-chain data. . Today, most decentralized applications handle media and assets with off-chain logic. They either use a cloud-based centralized solution like AWS S3 or Microsoft Windows Azure's storage service, or a decentralized solution like IPFS[9] or Swarm[10].

Rather than reinventing the wheel, we encourage application developers to adopt the best-fit solution for handling their media and assets. We predict that most application developers will use centralized solutions, which are the simplest and most mature. In addition, media and resources don't necessarily have any relationship with blockchain data in most applications. Other developers might consider using IPFS or a hybrid solution. ArcBlock allows you to decide which solution is best for your application—it works with either technological approach.

While the ArcBlock platform uses AWS to handle its own media and assets, we may consider moving toward a decentralized system in the future.

CLIENT LIBRARY/FRAMEWORK

ArcBlock provides libraries and frameworks for client application development. These libraries support web, iOS, and Android platforms. With the Electron Framework[11], the web version can be easily encapsulated and packaged as a desktop application for Windows and Mac OS.

9 IPFS (the InterPlanetary File System) is a new hypermedia distribution protocol, addressed by content and identities. IPFS enables the creation of completely distributed applications. https://ipfs.io

10 Swarm is a distributed storage platform and content distribution service, a native base layer service of the Ethereum web 3 stack. https://github.com/ethersphere/swarm

11 Electron is a framework for creating native applications with web technologies like JavaScript, HTML, and CSS https://electronjs.org

Archived copy · cryp2nova.com

The version for the web is a simple communication library that works with HTTPS and WebSocket to provide a real-time and reactive user experience. It works with nearly all other web frameworks, allowing you to pick the framework you'd like to work with, such as Meteor, VUE, or React.

This is an important advantage for application development. Engineers can spend most of their time handling the client side and user experiences, and write most of the code in this layer. Thanks to ArcBlock, however, now they can develop client applications the same way they build traditional, non-blockchain applications. Our design enables developers to work with their favorite frameworks and tools so they can draw upon community resources and support.

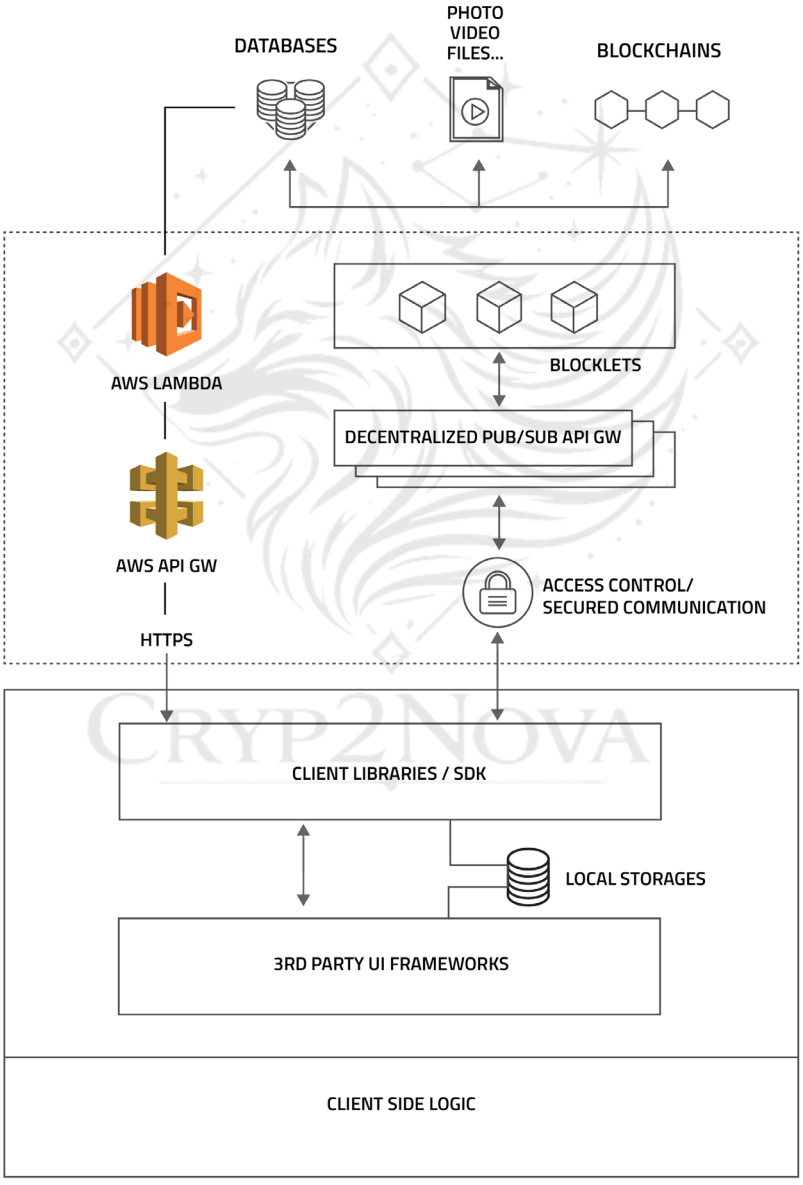


Fig: Client communication model of our reference implementation on AWS (as of Dec 2017)

Archived copy · cryp2nova.com

ALGORAND

ArcBlock is among the first blockchain startups to adopt Algorand[12] in production.

Algorand was founded by Silvio Micali, winner of the 2012 ACM Turing Award. Micali is a pioneer in cryptocurrency and blockchain technology. He was instrumental in the development of many of the building blocks of cryptography, published works on game theory and Byzantine Agreements, and even launched a micropayments startup. When Micali saw Bitcoin, he thought it could be improved; Algorand is the result of that quest.

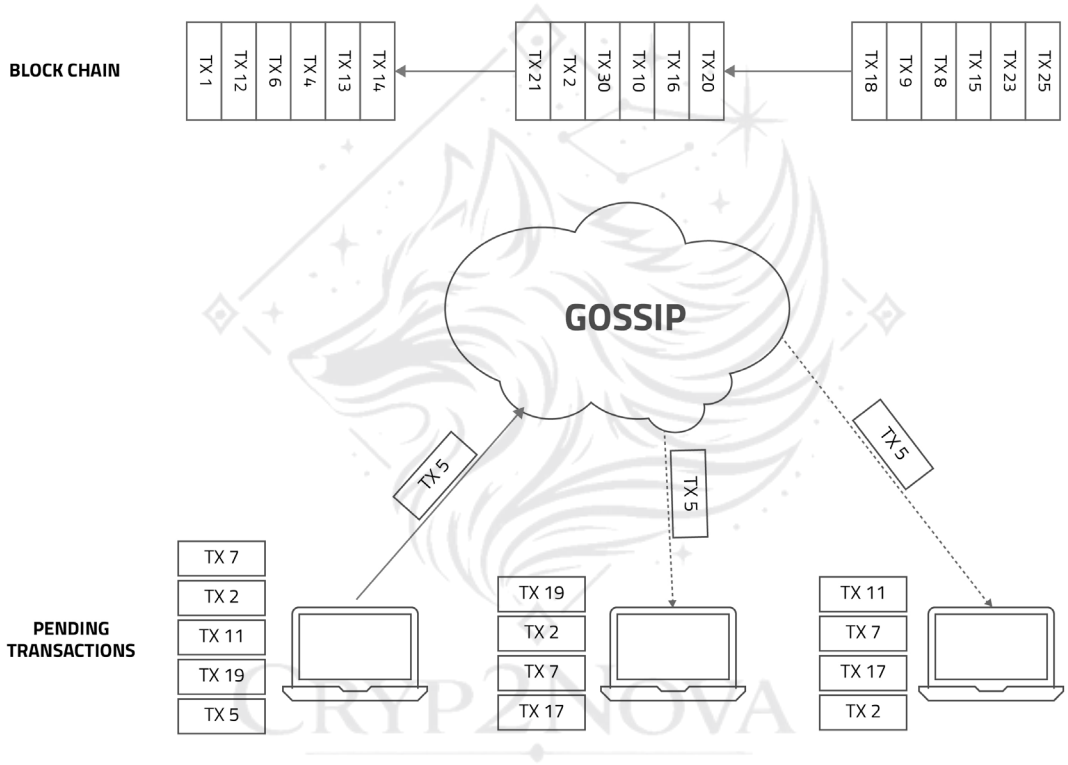


Fig: An overview of transaction flow in Algorand (via[13])

Algorand[14] involves suddenly and randomly selecting a small group of nodes to be in charge of the next block, then receiving a reward in the form of a percentage of the block transaction. This must be done in a way that can't be manipulated by an adversary. No one selects the group; it's selected by hash instead. Micali suggests taking a pseudo-random generator which is pre-specified and elongating as much as you need to select the committee. The group decides the next block via a redesigned Byzantine agreement in which a leader is picked randomly from the group.

12 Jing Chen, Silvio Micali, Algorand, Technical Report, 2017, https://arxiv.org/abs/1607.01341
13 Gilad et al., Algorand: scaling Byzantine agreements for cryptocurrencies, SOSP'17, https://people.csail.mit.edu/nickolai/papers/gilad-algorand.pdf
14 Algorand: scaling Byzantine agreements for cryptocurrencies, https://blog.acolyer.org/2017/11/21/algorand-scaling-byzantine-agreements-for-cryptocurrencies/

Archived copy · cryp2nova.com

ArcBlock uses Algorand and its variant in a number of places. For example, we use Algorand to pick where the smart contract Blocklet will execute from, as well as for the high-performance blockchain that powers our native tokens. We will disclose more details on implementing Algorand in the ArcBlock in the future when we reach release candidate milestone.

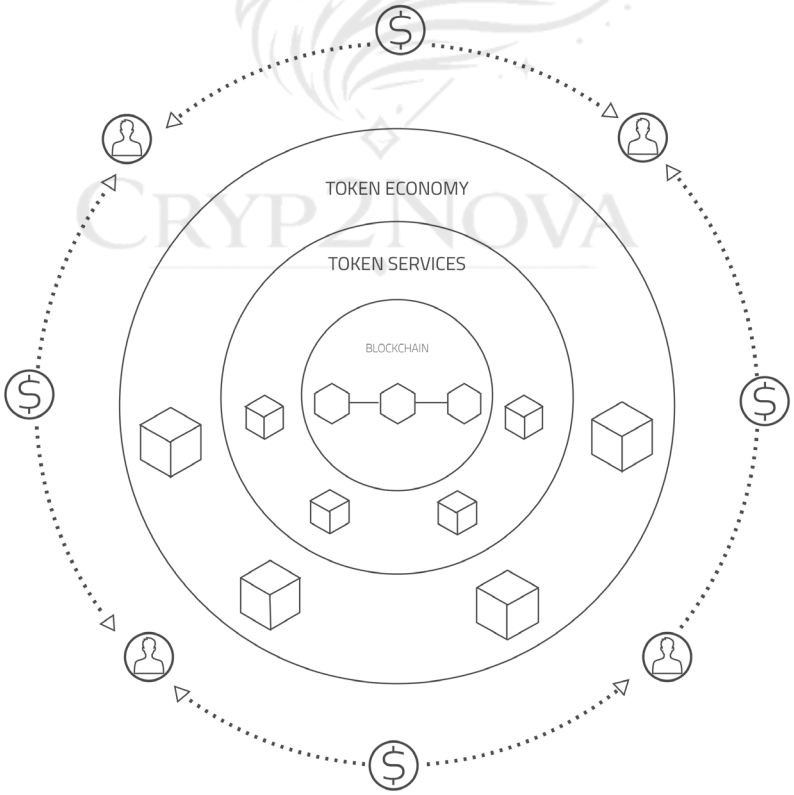
THE TOKEN ECONOMY AND THE SERVICE

What makes ArcBlock unique is that it's not just a set of APIs or libraries—it's a robust platform with a full set of features. In addition, the service runs on top of its own native token system, which is driven by latest blockchain technology.

THE ARCBLOCK TOKEN (ABT)

The ArcBlock Token (ABT) is native to the ArcBlock platform. To achieve high-performance transactions, we built an optimized blockchain dedicated to ArcBlock's own token services and the public ledger. The design goal is to achieve >100,000 Tx/s, which is more than adequate for a wide range of applications. In the future this blockchain could be improved for broader purposes.

The ARC is designed as a general purpose token that can be used in different scenarios. Within ArcBlock, the ABT's basic utility value is to pay for the cost of using the ArcBlock system. Like a cloud computing service, the ABT is a utility token for paying the cost associated with using the service.



Archived copy · cryp2nova.com

Unlike Ethereum or Bitcoin, where users typically pay a fee for each transaction they make, ArcBlock is designed to let application providers pay the transaction fees for their end users. This approach vastly improves the user experience. Developers pay on a monthly basis, enabling them to add up small units and save money. ArcBlock also request developers to lock in a number of ARC token as a stake when they need to provide mission critical services.

ArcBlock tokens map to ERC20 tokens 1:1. This simplifies token exchanges and allows developers to tie into the Ethereum community. Application developers can take advantage of the existing ecosystem built on the ERC20 token while also leveraging a high-performance and full-featured token service. While this mapping is necessary today, we anticipate that it may become obsolete as the ARC matures and the ArcBlock community grows.

THE MINERS

ArcBlock allow contributors ("miners") to run ArcBlock platform services and join the overall service network. The role of miners within the ArcBlock community is significantly different from that of Bitcoin and Ethereum contributors, however.

RESOURCE MINERS

Resource Miners contribute computing resources to the system. They might provide cloud computing resources and run as a cloud node, or contribute self-hosted computing resources.

In ArcBlock's design, Miners may provide the computing resources for their own use only, share them across multiple parties, or share them with anyone. The choice of model is entirely up to the miner, and can be changed as they need to.

COMPONENT MINERS

Component Miners contribute software components to the system, such as new Chain Adapters, Blocklet Components, or ready-to-deploy applications. The component might be packaged code that can be reused and deployed by another application, or a set of services that's merely exposed through the Blocklet interface. For example, a deep learning-based image recognition service may have its own services running elsewhere, but offer the services as Blocklets so that other ArcBlock applications can use them.

A smart contract defines how the miner's fee will be distributed if the component is developed by multiple parties. It will also define the rules for how the code for the component is forked.

THE ARCBLOCK MARKETPLACE

The ArcBlock Marketplace is a decentralized blockchain application built on ArcBlock platform itself. The app serves as a marketplace for listing, searching, evaluating, using, and ranking reusable components, such as Chain Adapters, Blocklets Components, and applications.

The marketplace is also responsible for maintaining public feedback about the quality of components and the reputation of their developers, as well as other information. This information will help users evaluate reusable components. All the marketplace information are recorded in the public ledger powered by ArcBlock's blockchain technology to ensure transparency and the trust.

Archived copy · cryp2nova.com

TOKEN FOUNDATION SERVICES

The platform's token foundation services consist of a set of Blocklet components that lay the groundwork for ArcBlock's token services.

The ArcBlock token is implemented entirely with Blocklet. The token foundation service is also powered by Blocklets, and the Token Economy Service consists of a group of Blocklet Building Blocks. Application developers can use Blocklet to easily handle events triggered by tokens and accomplish complex business logic. The distributed ledger in ArcBlock ensures that your tokens are secure, high performing, and reliable.

Just like any other Blocklet components, the Blocklets for the token foundation service can also be improved and extended by the blockchain community .

APPLICATION TOKENS

With ArcBlock, developers can also create their own custom tokens that inherit all of the features of our native token.

ArcBlock makes it easy to build your own economy. Tokens aren't just for cryptocurrencies, however. They can represent many different things, from user identities, certifications, and documents to real-world entities. ArcBlock enables you to tokenize everything in your application.

In the near future, you'll be able to make initial coin offers (ICOs) with ArcBlock's application token once you've built and deployed your applications with ArcBlock.

CRYP2NOVA

Archived copy · cryp2nova.com

ACKNOWLEDGEMENTS

This work is the cumulative effort of multiple individuals with the ArcBlock team, and would not have been possible without the help, comments and review from our partners, advisors, community collaborators and valuable customers.

This technical whitepaper was written by Robert Mao, the Chief-Architect of ArcBlock and reviewed by Flavien Charlon, the Chief-Scientist of ArcBlock. During the authoring process we received valuable helps and comments from the rest of ArcBlock engineering and marketing team, our partners, we also received lots of valuable feedback from the emails, WeChat groups, Telegram groups, conferences and forums.

We would like to thank all our advisors and collaborators for valuable conversations, in particular Ximen LiuShang, Justin Tomboulian, Violin Wang, Michael Yuan, Frank Lee, Richard Liu and Jonathan Lu. We woulds also like to thanks to Kate Dougherty and Jean Chen for the help on the proof reading and document structure.

- The End -

Copyright © 2017 ArcBlock Foundation Limited. All rights reserved. Draft for community review. Subject to change.

CRYP2NOVA

Archived copy · cryp2nova.com