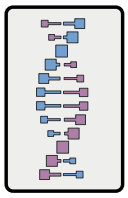

# duality

## blockchain solutions

whitepaper v0.1

Amir Abrams[1,2], Bernhard Altaner[3], Spencer Lievens[1], and Mark A. Schroeder[4]

[1] *Duality Blockchain Solutions*
[2] *HarmonIQ Health Systems*
[3] *University of Luxembourg*
[4] *Ubiquitous Solutions*

November 9, 2016

Blockchain technology enables reliable and secure organization of decentralized networks without any single point of failure. Most public and private organizations require collaboration and data exchange between different structures with many institutional and private participants. Often, services require the secure identification of a user, which ultimately needs to be matched with associated personal data that is distributed amongst various databases. Ensuring the accessibility of such data while complying with strong privacy requirements is a difficult task. In the context of health care, the efficiency of this process can be a matter of life or death.

As a solution to these problems, in this paper we present the *duality* platform. As implied in its name, *duality* leverages a binary architecture consisting of the *dynamic* blockchain as a decentralized autonomous organization and the *sequence* blockchain as its real-world interface. In particular, we describe *duality*'s patient identity service (*noID*) for health care as our first solution. In addition, we outline the potential of *duality*'s ecosystem to offer a variety of powerful business services, which were infeasible before the advent of blockchain consensus technology.

# Contents

# 1. Introduction

The purpose of this early whitepaper is to present *duality*, a binary blockchain platform developed by Duality Blockchain Solutions Ltd. (DBS), a for-profit organization based in the UK [1]. The vision of *duality* is to apply blockchain technology to real-world problems. In order to achieve this goal, *duality* leverages the advantages of both permissionless and permissioned blockchains. While blockchains provide the technological backbone of our solutions, end-users and participating organizations do not need to understand the details of *duality*'s architecture. In order to use *duality*, end-users simply log-in their duality profile at points of service or via a web interface. Participating organizations can purchase *duality* credits to register these profiles for their end-users.

In this paper, we give an overview of *duality*'s architecture and its health care solution, *noID*. On the lowest level, duality is based on two independent blockchains executing different tasks for the *duality* platform. The first chain, *dynamic*, is a permissionless public blockchain which focuses on privacy, anonymity and efficiency. In order to achieve these goals, the *dynamic* chain makes strong use of the recent technological innovations in the field. Using a second tier of specialized network nodes, *dynamic* aims to establish a decentralized autonomous organization (DAO), which self-governs its evolution in a sustainable manner. The second chain, *sequence*, provides *duality*'s interface to the real world. Like *dynamic*, *sequence* has two tiers of nodes. Regular nodes sustain the basic functionality of the blockchain, whereas specialized nodes cater to the needs of a specific real-world problem. Unlike the permissionless *dynamic* chain, *sequence* features a novel hybrid model, where regular nodes are run by the public, while the application-specific specialized nodes are licensed to customers by DBS.

The first such application, the *duality noID* solution, targets the health care sector. It provides an accurate, reliable and fast solution for identifying patients and enabling secure access to their protected health information (PHI). While the efficiency of patient identification and data retrieval can be a matter of life or death [2], so far no satisfactory and scalable solution to this problem has been found. We will show in detail below, how *noID* suffers from none of the issues faced by current systems and can be easily integrated into existing systems. Its initial implementation will focus on and comply with the public health care system in the United States. However, *noID* is designed to be easy adapted by health care organizations throughout the world and we expect *noID* to be deployed on a large scale in the near future.

This work is structured as follows: In section 2 we give an overview of the architecture of the *duality* chains and their interactions. Our solution to health care, *noID* is described in detail in section 3. An outlook focusing on future developments and the sustainability of the system is presented in section 4, before we conclude this work in section 5. Technical details about the *duality* protocol and its implementation are given in the appendices.

# 2. Architecture Overview

In this section, we give a high-level review of *duality*'s binary architecture, focusing on its two chains and their internal and external communication structure.

## 2.1. The *dynamic* Blockchain

The *dynamic* blockchain is a privacy-centric blockchain and serves as *duality*'s main communication infrastructure. Network nodes can be run by anyone without any special requrirements. Contributions to the network are rewarded by means a proof-of-work (POW) consensus protocol implementing the Argon2D algorithm [3]. Participating nodes are rewarded `DYN`-credit, which is a cryptographic utility token necessary to use the features of *dynamic*. Specialized second-tier nodes (so-called *dynodes*) act as communication relays for the *duality* protocol. Besides their role as ID Hubs that store *duality* profile data (see below and section 3), they facilitate the governance structure of the *dynamic* DAO.

The idea of *dynodes* is derived from DASH's masternodes [4, 5]. Like masternodes in DASH, *dynodes* need a certain amount of `DYN` as collateral to prevent abuse. For their services, *dynodes* earn `DYN` as the state of the chain progresses. Moreover, good behaviour like timely query responses, high availability and good trust relationship management results in higher *dynode* rewards, thus generating an economic incentives for efficient operation.

## 2.2. The *sequence* Blockchain

The second constituent of *duality*'s binary architecture is the *sequence* blockchain. Similar to *dynamic*, it has two tiers of nodes. Regular nodes can be run by everyone and propagate the blockchain by agreeing on the next valid block. Unlike *dynamic*, the consensus mechanism is not based on proof-of-work but on proof-of-stake (POS), using Peercoin's [6] POS-algorithm [7]. Block rewards are paid in *sequence*'s own `SEQ` tokens.

Specialized nodes on the *sequence* chain (so-called *seqnodes*) act as interfaces to the real world. They run application-specific software and cater to participating public and private organizations. In order to prevent third parties from interfering or fraudulently impersonating a participating organization, *seqnodes* are permissioned. This means, they require a unique cryptographic certificate issued using the blockchain against a recurring fee. For any given application, DBS will provide an open-source stand-alone open-source reference implementation (RI, hosted on *GitHub*[8]), which supports all protocol node types and all functions of the system. In addition, DBS may offer integration into existing IT systems as a paid service.

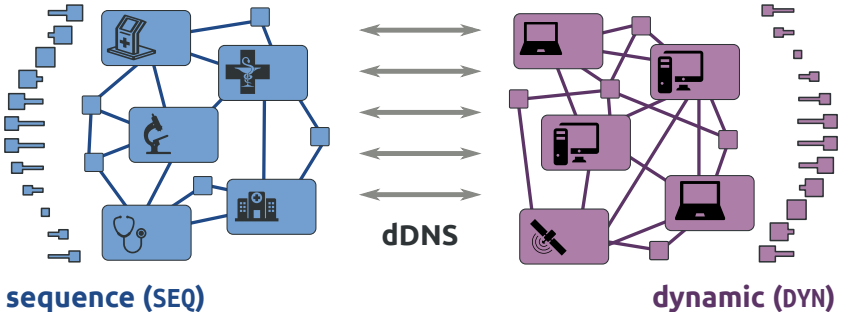


Figure 1: The duality binary blockchain with its two independent subchains, *sequence* (left) and *dynamic* (right). Both chains are public blockchains with their associated cryptographic tokens `SEQ` and `DYN`. *duality* functions are facilitated by specialized nodes: licensed *seqnodes* on *sequence* and collateral-backed *dynodes* on *dynamic*. Secure inter-chain communication is routed via a dDNS service.

## 2.3. The *duality profile*

Interfacing with the real world means interfacing with real people. In order to correctly retrieve or display user-specific data, it is crucial to accurately verify the identity of a person. In the context of health care such data may be protected health information (PHI), whereas in the context of finance or trade this could be, for example, bills, orders or credit card data. As such, each end-user of *duality*'s platform has a unique *duality profile*, containing data that uniquely identifies the real-world person behind the profile. Besides this personal data, a user's *duality profile* contains a set of user-specified privacy preferences (a user's sharing profile), which limit or grant access to associated sensitive data. More precisely, a *duality profile* contains a cryptographically abstracted (hashed [9]) watermark of the data, ensuring that this data has no meaning outside of the *duality* environment. For increased security and reliability, profiles are stored redundantly on *seqnodes* and *dynodes* across both chains, thus eliminating any single point of failure.

## 2.4. Intra- and Inter-Chain Communication via dDNS

The communication amongst specialized nodes, both within and across chains, relies on a decentralized Domain Name Service (dDNS [10]). A public/private key infrastructure (PKI) ensures the security of this communication and prevents spoofing attacks by third parties. All registered node names/public keys are discoverable through a *duality* blockchain audit procedure. For enhanced security and anonymity, clients can interface with the *duality* dDNS using Tor [11] in addition to ClearNet services.

# 3. *noID*: fixing health care

In this section, we demonstrate how *duality* acts as an accurate, secure and fault-proof solution in the health care environment. More details on that can be found in a more specialized version of this document [12].

## 3.1. State of the Art

As of today, there are several existing protocols and standards such as HL7 (HL7 FHIR, HL7 CDA, HL7 2.x [13]) and Direct Messaging [14] which enable the sharing of clinical data among health care providers. However, the inability to accurately and securely identify patients across environments hinders the efficient use of the existing standards. Moreover, even if a patient is correctly identified, it is not guaranteed that all relevant information (protected health information, PHI) can be located and retrieved efficiently.

## 3.2. Using *duality*

The *duality* Binary Blockchain and its associated protocol allows for uniquely identifying people in various contexts. Here, we apply the concept of *duality* to patient identification, with a focus on health care in the United States. Besides using classical forms of identification (like ID, driving license), *duality* can accurately identify patients by means of biometric data (fingerprint minutiae, in the future possibly DNA). This *noID* functionality is of particular importance in emergency situations. Moreover, *duality* does not exclude people lacking official identification documents and thus ensures a fair access to health care for everyone, regardless of sex, social status or nationality. The storage of *duality* profiles across two complementary blockchains excluding any single point of failure. Using biometric data in addition to hashed demographic data allows patients to be correctly identified with virtually 100% accuracy.

At any time, patients may audit or update their access preferences (sharing profile). The concept of a patient-managed sharing profile changes the clinical data sharing paradigm by putting the patient (or their delegate) in control of protected data. *duality* thus alleviates the health care organization's responsibility and risk when engaging in clinical data exchange. Moreover, patients can opt-in to have some of their data shared with research institutes in anonymized form. Thus, *duality* creates a self-governing ecosystem that lowers the overhead and complexity of the current Health Information Exchange (HIE) interoperability model [15] by eliminating the need for complex inter-organizational legal data use and sharing agreements.

In contrast to other proposed blockchain-based health care proposals, a patient's PHI is never stored on the blockchain, minimizing the risk of data breaches. *seqnodes* exchange data using the existing industry standards (HL7 FHIR), while the requests between *seqnodes* are relayed

through the privacy mechanisms implemented by *dynodes*. This excludes the possibility of third parties to identify or expose patients by means of communication metadata.

## 3.3. Scalability and Adaptability

The scalability of the *duality* protocol is one of its most robust aspects. Because a *duality* Profile of hashed biometrics and demographics is used for patient identification, there is no logical limit on the number of unique *duality* patient resources which can be created and managed. We expect this to be true now and well past 120 years from now, and true for 100% of the US population if they are willing to enroll and have access to a *seqnode*. The primary limits to the number of patients the *duality* protocol can handle are set by patient access to participating Health Organizations, rather than logical scalability. However, the barriers for organizations to enter the system are so low that any entity involved in patient care can easily join and participate in *duality*. The *duality* protocol is designed to use open source software, operate on multiple software platforms, and employ commodity hardware to help facilitate easy and inexpensive node and hub registration (See Appendix B).

The *duality* protocol is capable of handling any patient regardless of socio-economic or cultural background. For the standard health care provider, such as an ambulatory clinic or pharmacy, facility based protocols for managing non-US citizens would be employed. However, *duality* does not require any demographics which are specific to nationality, so any issues relative to non-English speaking or non-US citizens would be relegated to providing meaningful feedback to the patient by an Health Organization's *seqnode*. Additionally, we believe that the *duality* protocol is ultimately capable of interfacing with other projects which leverage similar biometrics such as the "Aadhaar" project in India [16]. However, this type of interfacing is beyond the scope of this paper.

*duality* implements a scalable technical architecture with built-in clustering, high availability, fast performance, low maintenance, and easy administration/setup with efficient utilization of computer resources. When data is transmitted over the wire, *duality* utilizes protocol buffers [17] to reduce data packet size and memory utilization. *duality* will also be able to integrate with other network protocols like Libtorrent [18] and/or Facebook's Warp speed Data Transfer(WDT) [19] to increase efficiencies over high latency connections.

The *duality* protocol does not leverage a central repository to house patient PHI, but instead facilitates how Health care Organizations exchange the PHI that they house and protect. The framework uses HSPC [20] standard HL7 FHIR messaging protocol [21]. *duality* applications will be HSPC certified and participate in their app store ecosystem [21]. The HL7 Patient Resource serves as a standard, which allows for the exchange of patient data with any system which is capable of consuming these standard messages.

IT systems such as Electronic Health Records will also need to adopt the open source protocols to integrate with *duality*. However, organizations can use the standalone open source reference implementation software without integrating into their IT system (See Appendix A: Reference Implementation). The *duality* solution will cause a high percentage of patients of

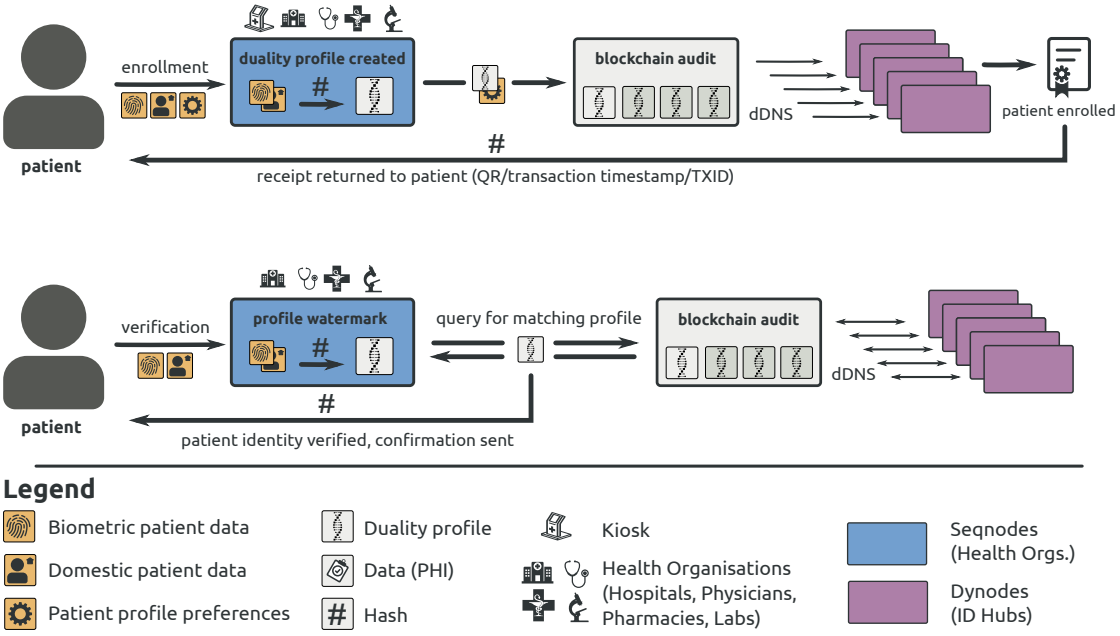


Figure 2: Patient enrollment and verification procedure.

all types to participate due to its adoption by the greater health care community. Compared with other possible solutions, *duality* is open source (i.e., free), nonproprietary software that runs on commodity (i.e., inexpensive) hardware. Lastly, the solution is crossplatform and capable of running on the vast majority of existing operating systems (See Appendix B: Basic Requirements).

## 3.4. *duality*'s *noID* Protocol

Patients interact with the *duality* infrastructure using *seqnodes* available at points of care (hospitals, pharmacies, physicians, labs), at specialized health care kiosks of using a web-interface. *seqnodes* then use *duality*'s dDNS system to obtain the data associated to a *duality* profile from specialized *dynodes* acting as ID Hubs. In case PHI is requested, the requesting *seqnode* obtains the dDNS address of the *seqnode* associated with the database containing the PHI. PHI exchange between *seqnodes* uses established industry standards and never exposes any sensitive data to the blockchain. The different tasks handled by *duality* protocol are listed below. For more technical details, see Appendix B.

### Enrollment

Patients enroll into *noID* by presenting themselves to *seqnodes* at points of care or using a smartphone, PC or kiosk running the *duality* RI software with a fully downloaded blockchain.

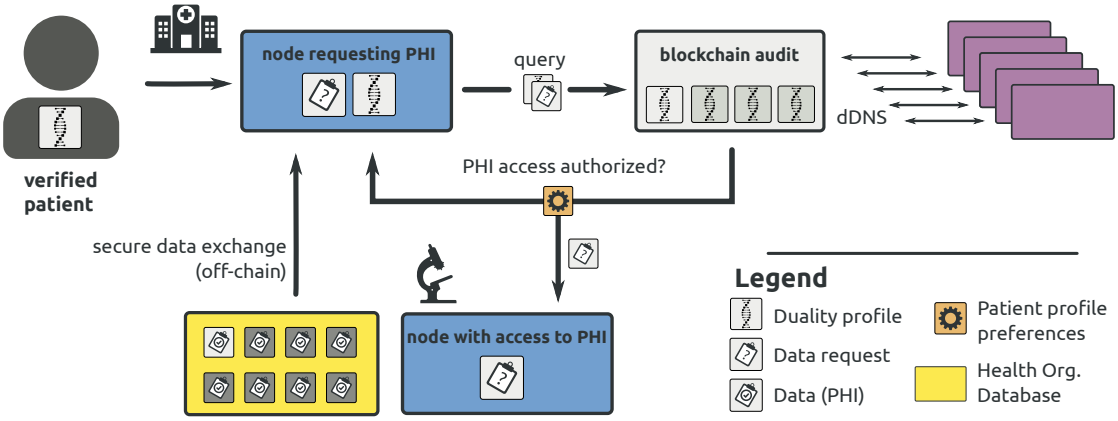


Figure 3: PHI exchange.

There is no direct enrollment fee for patients and any patient can only enroll once. The *seqnode* then collects demographic and biometric information to form the *duality* Profile used for authentication and matching (see Fig. 2). To secure the account, the patient selects an unlock pattern on top of a custom image. Further, the patient can delegate authority to other *duality* profiles if they can not manage their own account. When enrollment is successful, the patient receives a receipt as a confirmation.

### Verification

A patient presents themselves at a point of care, where a *seqnode* captures some biometric information from the patient. This information is then checked against existing *duality* profiles, both locally at the *seqnode* and, if necessary, via a query to a regional *dynode* acting as an ID Hub. If a match if found, a medical record location message is returned to the *seqnode* at the point of care (see Fig. 2).

### Data exchange

After a patient is identified, the *seqnode* receives a list of medical record locations that can be used to initiate clinical data exhange. With the patient's authorization defined by their *duality* profile, a health care *seqnode* can request data from another *seqnode* on the secure *duality* network. An encrypted connection between the *seqnodes* is established using existing industry standards for clinical data exchange (see Fig. 3). *duality* further facilitates data exchanged by embedding Restful FHIR services and data transformation tools. Data exchange between *duality* nodes is always secure and private; PHI is never stored on its public blockchains.

#### Profile audit and management

Patients can audit their *duality* Profile via a secure website using the unlock pattern created at enrollment. This website provides meta-data about the patient's *duality* Profile such as which nodes matched on their Profile, what data element may have been updated, date/times of any actions related to their profile, and contact information for *dynodes*.

# 4. Outlook

## 4.1. Decentralized Pharmacies

Already today, online pharmacies that deliver orders to customers through the mail or shipping companies are a billion dollar market. However, the sale of prescription-limited drugs comes with strong regulatory requirements. In *duality*, prescriptions can be issued to patient profiles by licensed health care organizations. Authorized vendors can verify a patient's prescription and report the fulfillment of a drug order to *duality*, ensuring that no prescription can be redeemed multiple times. The privacy features of the *dynamic* chain ensure that no third party (like hackers or unauthorized users) can aggregate a patient's prescription history.

## 4.2. Future *sequence* development

While patient matching for the health care industry is *duality*'s first solution, the potential of the platform is virtually unlimited. DBS will continue to develop existing solutions like *noID*, but also reach out to other public and private organizations that are in need of scalable and secure decentralized solutions.

## 4.3. Viability of the *dynamic* DAO

Having strong incentives for the public to use and sustain the *dynamic* chain ensures the viability of *duality*'s communication infrastructure. To that end, the *dynamic* chain is equipped with a dynamic self-governing structure enabling a decentralized autonomous organization (DAO). In regular intervals, the *dynamic* chain issues a budget in `DYN` tokens which can be used to fund further development. Operators of *dynodes* are able to vote on the allocation of this budget in a fair and anonymous manner. This perpetual funding structure will secure the viability of the *dynamic* chain, thus ensuring its sustainability. For more details, we refer to the DASH DAO [4, 5].

# 5. Conclusion

In this paper we have outlined the architecture and the first use case of the *duality* platform, which leverages blockchain technology to provide decentralized solutions for real-world problems. We discussed the robustness, security and adaptability of the platform, which makes it attractive to public and private organization acting on a large scale. We presented *noID* as *duality*'s fully developed solution to patient identity verification and clinical data exchange, which complies with all regulatory and technical requirements for health care in the US. While *duality* relies heavily on modern cryptographic technology, the complexity of the system is hidden to end-users and participating organizations, thus achieving very low barriers for entry to the system.

# A. *duality* Protocol Definitions

- *duality* Blockchain:
  Two decentralized, consensus driven immutable public ledgers that securely stores credit inputs/outputs (wallet balance), *duality* fees, *seqnode* and *dynode* registration, budget proposals, budget votes and ID HUB quality votes. These blockchains are implemented and based on the original blockchain protocol [22].
- Reference Implementation (RI):
  The *duality* open source protocol reference implementation software is hosted publicly on github [8]. The core implementation supports all protocol node types and all functions of the system.
- *duality* P2P Network:
  A peer to peer network of nodes running the *duality* RI software. The P2P network enables nodes to securely communicate and share the public *duality* blockchain.
- *seqnode* (Health care Organization Node on the *sequence* blockchain):
  A registered name/public key pair that represents a health care organization on the *duality* blockchains. A decentralized name registration or dDNS will be implemented much like Emercoin [10].
- Sharing Profile (*duality* profile privacy preferences):
  A hashed patient resource used to store and transmit patient privacy and security settings.
- *dynodes* (ID Hubs):
  An ID Hub run on a *dynode* is a specialized second tier node responsible for patient record location and patient security profile services. It stores biometric and demographic hashes for match verification. All *dynodes* maintain a list of trusted health care organization nodes. They must maintain a collateral wallet address. Its credit balance dictates how many patients they can host on the *duality* network. These nodes will be implemented much like DASH's masternodes [5] and also use dDNS name registration on the blockchains.
- Node Trust Template:
  List of *seqnodes* trusted by a *dynode* used in a patient's default privacy and security settings.
- *duality* Profile:
  A resource containing hashes that represent a patient's demographic and biometric information used for matching.
- *duality* Digital Tokens (`SEQ` and `DYN`):
  The integrated credit system is used to pay for patient matching queries, collateral, *seqnode* and *dynode* name registration fees, storage, and patient location services.

- *dynode* Quality Votes:
  Each match fee paid by a Node entitles them to 1 quality vote in the next monthly quality budget superblock cycle.
- Budget Proposal Votes:
  *dynode* can vote on foundational project budgets that are paid monthly with a superblock cycle. Project budgets are used to fund protocol and foundation development.
- Sharded Cache Nodes:
  Specialized decentralized *duality* nodes used to store shards of encrypted *dynode* cache data. These nodes work much like the MaidSafe's SAFE network [23] to protect from decryption, unauthorized access and data loss.
- *duality* Certificates:
  These certificates are created during *dynode* and *seqnode* registration process and contain all the information and keys needed to run a registered *duality* node or cluster.

## B. Protocol Set-up and Configuration Workflows

- Basic Requirements:
  Internet connected *duality* approved biometric device running the *duality* RI software. All major Smartphone, Kiosk, and Desktop platforms supported.
- *dynode* Setup: To register a new ID hub (*dynode*) on the blockchain, basic information is entered, a collateral wallet is created and a hub registration fee is paid in *duality* credit. This is a list of the required information:
  - Public Key Address
  - Private Key Associated with Public Key Address.
  - *dynode* Name Associated with Public Key Address
  - *dynode* ID Hub Patient Portal Page
  - Challenge/Response page URL. Verifies your system can decrypt using the public key registered in the blockchain.
  - System Admin Contact group of *duality*
  - Compliance Office group *duality*
  - Send coins to collateral wallet address.

  Each hub node needs access to a Couchbase Server NoSQL cluster [24] that securely stores *duality* resource hashes for their patient accounts. All PHI required by the hub UI is stored by Sharded Cache Nodes.

- *seqnode* Setup:
  - Register name on the blockchain with basic organizational information and a node registration fee.
  - Required Information:
    * Public/Private Key Pair
    * Health care Organization Name
    * Organization Domain URL
    * *seqnode* Type (Pharmacy, Hospital, Small Doctor's Office, etc.)
    * Challenge/Response page URL.
    * Facility Address
    * List of primary contact phone and email
  - Optional Information:
    Communication Server URL
- Patient Enrollment:
  There is no enrollment fee to be paid by patients. A patient can enroll using a smartphone, PC or kiosk running the *duality* RI software with a fully downloaded blockchain. The device(s) collects demographic and biometric information, downloads the hub hash template and creates hashes to form the *duality* Profile used for authentication and matching. To secure the account, the patient selects an unlock pattern on top of a custom image. A patient can only enroll once in the *duality* system. The patient can delegate authority to other *duality* profiles if they can not manage their own account like in the case of children.
  - Required Demographics Hashes:
    Full Name, Date of birth, Gender, City, State
  - Biometrics Template Hashes
  - Optional Information Hashes:
    Street address, ZIP code, phone number, name of parents, name of children, name of siblings, driver's license number, insurance policy numbers, race/ethnicity, blood type, chronic diseases, birth order.
- *dynode* (ID Hub) Access:
  The patient can access the account associated to their *duality* profile by using the *duality* RI software. At least one biometric reading and the correct unlock pattern is needed to authenticate. Once authenticated, the user can modify default sharing profile, anonymity settings, demographics, and all other settings to manage their hub account. The hub also stores audits collected from *seqnode* match requests.

- *seqnode* to *seqnode* Communication:
  All registered *seqnodes'* names/public keys are discoverable using the *duality* blockchain. Nodes can securely communicate by sending *duality* resources and encrypting them using the recipient's public key.
- *seqnode* to *dynode* ID Hub Communication:
  To conduct patient matching, nodes send the captured *duality* profile to regional ID Hubs. If there is a match, a response is sent back to the node with record location information and the patient's sharing profile.
- *dynode* to *dynode* Communication:
  ID Hubs need to communicate to transfer patient accounts. Hubs can also propagate *duality* Profile changes to other Hubs (i.e., due to need to rehash data).
- Patient Verification Process:
  - Patient presents at *seqnode*, and the node captures at least one biometric from the patient and creates a preliminary *duality* profile.
  - The *duality* software checks for an internal *seqnode* match
    * If an internal match is found, the user must confirm the match.
    * If a match is not found, the *seqnode* user selects or enters the patient demographics. Demographics can auto-populate a node via a typical registration resource interface. *duality* uses a REST RPC API to send and receive *duality* patient messages within their intranet.
  - The *seqnode* sends the patient's full *duality* profile to regional ID hubs for matching. A fee is paid to the network to conduct the match.
    * If a match is found, a *duality* resource is returned containing record location pointers and the patient's sharing profile.
    * If a match is not found, the fee is refunded and the node user should follow the patient enrollment procedures if possible.
- Patient Audit Process:
  Patient can audit their *duality* Profile via a secure website using the unlock pattern created at enrollment. This website provides metadata about the patient's *duality* Profile such as which nodes matched on their Profile, what data element may have been updated, date/times of any actions related to their profile, and contact information for *dynodes*. However, no PHI is available for download or viewing via this site. This interface also displays the *duality* privacy and security settings for review and/or modification.

# References


[1] "Duality Blockchain Solutions Ltd." [Online]. Available: https://beta.companieshouse.gov.uk/company/10435961

[2] M. A. Makary and M. Daniel, "Medical error—the third leading cause of death in the US," p. i2139. [Online]. Available: http://www.bmj.com/lookup/doi/10.1136/bmj.i2139

[3] A. Biryukov, D. Dinu, and D. Khovratovich, "Argon2." [Online]. Available: https://password-hashing.net/submissions/specs/Argon-v3.pdf

[4] E. Duffield and D. Diaz, "Dash whitepaper." [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper

[5] Masternode budget API - official documentation. [Online]. Available: https://dashpay.atlassian.net/wiki/display/DOC/Masternode+Budget+API

[6] S. King and S. Nadal, "Peercoin - secure & sustainable cryptocoin." [Online]. Available: https://peercoin.net/whitepaper

[7] P. Vasin, "BlackCoin's proof-of-stake protocol v2." [Online]. Available: http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[8] github.com. [Online]. Available: https://github.com

[9] Cryptographic hash function. Page Version ID: 744983266. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=744983266

[10] Emercoin International Development Group, "EMCSSL -decentralized identity management, passwordless logins, and client ssl certificates using emercoin nvs." [Online]. Available: http://emercoin.com/content/EMCSSL.pdf

[11] Tor project: Overview. [Online]. Available: https://www.torproject.org/about/overview.html

[12] A. Abrams, M. A. Schroeder, and S. Lievens, "Duality healthcare," 2016.

[13] Health level 7. Page Version ID: 740206104. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Health_Level_7&oldid=740206104

[14] The Direct Project. Direct messaging. [Online]. Available: http://directproject.org/

[15] HealthIT.gov. Health information exchange (HIE). [Online]. Available: https://www.healthit.gov/HIE

[16] Aadhaar project. [Online]. Available: http://uidai.gov.in/aapka-aadhaar.html

[17] Protocol buffers - a language-neutral, platform-neutral extensible mechanism for serializing structured data. [Online]. Available: https://www.google.com/protocol-buffers

[18] libtorrent. [Online]. Available: libtorrent.org

[19] Facebook warpspeed data transfer. [Online]. Available: github.com/facebook/wdt

[20] hspconsortium.org. Healthcare services platform consortium. [Online]. Available: https://healthservices.atlassian.net/wiki/display/HSPC/Healthcare+Services+Platform+Consortium

[21] FHIR Infrastructure Work Group. FHIR - Fast Healthcare Interoperability Resources. [Online]. Available: https://www.hl7.org/fhir/

[22] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." [Online]. Available: https://bitcoin.org/bitcoin.pdf

[23] David Irving et. al. Maidsafe whitepapers. [Online]. Available: https://github.com/maidsafe/Whitepapers/tree/gh-pages/pdf

[24] couchbase.com. Couchbase nosql database. [Online]. Available: http://www.couchbase.com/nosql-databases/couchbase-server