Hydro Snowflake: Decentralized Identity Management

June 2018

Table of Contents

Abstract

Hydro’s mission is to become the public ledger for financial services, empowering a new decentralized global economy. This ecosystem consists of standard smart contracts that can be used by financial applications, connected through APIs. These standardized smart contracts and API connections reduce the need for firms to hire blockchain developers and allow them to add decentralization to existing systems.

A core component of the financial ecosystem is the notion of identity and identity management. It is vital to creating security for account opening, transactions, payments, and trillions of dollars of global financial activity. With the growth of digital commerce, identity management becomes even more crucial to the future economy.

In this paper, we propose a new paradigm for identity in financial services that leverages a public and decentralized blockchain, called Snowflake. Users own their Snowflake identities, they are immutable, and they can be validated. Each Snowflake identity is tied to cryptography embedded in the user's mobile device, which is connected to a unique ID on the blockchain. This identity can be shared with third-parties at the discretion of the user, and creates the groundwork for Hydro’s future privacy management protocol.

This proposed identity platform can help to solve multiple problems:

1. Paper-based identity management is currently expensive and prone to theft and hacks
2. The dark web has increased the profitability for stolen identities
3. There are no global open standards for identity management, and private blockchain initiatives are making the problem worse
4. E-commerce and digital banking has made it increasingly difficult for companies to confirm their users’ identities
5. Emerging economies fail to utilize the growing use of mobile phones to their advantage in identity creation and management

Hydro’s Snowflake can create a global standard that complies with private and sovereign KYC standards, while empowering billions to own and secure their personal identities. This has implications for instant account onboarding, global ID passports, and when combined with the Hydro Raindrop, near zero credit card and bank fraud.

Background

The Origins Of Identity

In our first Whitepaper, we examined the the need for proper authentication of users within a technology ecosystem. Yet, authentication is not sufficient if there has been nothing identifiable to authenticate. In this whitepaper, we examine the urgent need for a better identity management framework that can be applied across financial services. Before exploring how a public blockchain can provide the missing piece to this puzzle by making identity immutable and standardized, let us first examine a more fundamental question: what is identity and where does it come from?

It is believed by scientists that names, the most fundamental forms of identity, pre-date the written word, originating perhaps as soon as humans gained the ability speak. There is even compelling evidence that other mammals, such as dolphins, establish "identities" using signature whistles as naming conventions for one creature versus another. As with humans, these identities help to forge tight communal relationships among mammals.

The idea of governments formally tracking names, via birth certificates, is a relatively modern one. For years, births and naming were a church function in most western societies. During the immigration wave in the U.S. of the 1800s, which brought 30 million immigrants, reformers pressured the U.S. government to formally track births and deaths in the census, but it wasn't until World War II that standardized birth certificates establishing where you were born and what was your name became mandatory in the U.S.

Yet, formally establishing these basic pieces of information is not enough to establish a unique identity. From the earliest time, surnames were used to establish what was your occupation, or who your parents were. The surname Smith was applied to blacksmiths, Robertson was the "son of Robert," and Bin Ali was the "son of Ali." The commonality of surnames makes identity management incredibly challenging. According to Ancestry.com:

> Most of the approximately 100,000 Japanese surnames in use today only date from 1868, when surnames were mandated for the first time, There are just a few hundred common Chinese surnames, and 20 of them are shared by half the population. There are about 250 Korean surnames, three of them comprising almost half the Korean population, and just about 100 Vietnamese ones, with three making up 60 percent of all names in that country.

In the United States, Smith is the most common surname in 40 of the 50 states. Because of the commonality of names worldwide, proper identity management necessitated governments to start national identification numbers.

National Identification Numbers

In the U.S. the Social Security number (SSN) was created in 1936 for the sole purpose of tracking the earnings histories of U.S. workers, for use in determining Social Security benefit entitlement (after the adoption of the Social Security Act in August 1935) and computing benefit levels. Names and addresses were considered, along with fingerprints, but names encountered many of the same concerns with commonality raised previously, and in the 1930’s fingerprinting was most associated in the United States with criminal activity.

There are nine digits in the U.S. SSN. The first three digits are assigned by geographic region or zip code, and the middle two numbers are group numbers that further identify the geography, while the last four numbers are random serial numbers. Thus, it is common for businesses to confirm only the last 4-digits of the number for identification purposes, making these numbers extremely prone to theft.

Likewise, many other countries have similar national identification numbers, sometimes called Social Insurance Number, Tax Identification Numbers, or National Identification Numbers.

Black Market For Identity

Because identities are not immutable, and many governments and private actors in the ecosystem cannot be trusted to create or confirm identity records, there is a thriving black market for fake and forged documents. Take for example, a Cuban birth certificate. To an illegal immigrant in the U.S. having a Cuban birth certificate could mean a path to citizenship in only 1 year, so those forged birth certificates have been sold for $10,000 or more.

It has also been estimated that up to 40% of the passport fraud in the United States involves counterfeit or stolen birth certificates from Puerto Rico, and Security Alliance reports that in 2008, 45,622 children were born in Puerto Rico, but in that same year 860,000 certified copies of birth certificates were issued! The current government identity system is severely broken, it incentivizes bad actors both in the private and public sector, but also creates a black market that incentivizes impoverished populations to sell their identities for extra income.

With this in mind, how can we expect to have a fair and honest financial ecosystem? Banks, credit card companies, and even startups struggle to properly identify users, and even when they do, is there ever a way to truly know if the person is who they say they are?

Identity Theft & E-Commerce

As examined in our Raindrop Whitepaper, identity theft is a growing problem in the U.S. and worldwide. In April 2017, Symantec published its Internet Security Threat Report, which estimates 1.1 billion pieces of PII (personally identifiable information) were compromised in various capacities over the course of 2016. Commerce is increasingly done remotely, and this lack of personal contact has made financial fraud easier to perpetrate, and harder for authorities to stop. There is no identification required for the vast majority of online transactions. It is based on a system of “trust” and that there will be a certain percentage of chargebacks and fraud cases that are written off. The average cost of chargebacks alone is approximately 1.47% of a merchant’s yearly revenue, and $118 billion in lost sales occur during false positives - when a merchant stops a legitimate customer from making a purchases because they falsely identified them as a fraudster. These are staggering figures that can easily be solved with immutable IDs tied to the public blockchain that are used during credit card and e-commerce transactions.

Current Forms of Identity

The overall concept of identity is changing as we approach the Web 3.0 and will continue to evolve over time with the advent of more artificial and sentient intelligence in global society.

Identities currently take two common forms - private and public.

- Private identities are things like telephone numbers, and email addresses.
- Public identities are things like tax identification numbers, passport numbers, and other forms of identification that are formed within civil societies.

Increasingly, research has shown that private forms of identities have begun to tell us more about ourselves, and produce more emotional attachment than public forms. Many have argued that a cell phone number has now replaced a Social Security Number in the United States in importance. According to Statista, global cell phone users are expected to reach 5 Billion in 2019, with over 50% using smartphones.

An example of the longevity and utility of cell phone numbers can be found in the U.S. mobile to mobile porting stats. In 2003, the first year data was collected, only 795,000 numbers were in the U.S. mobile porting database, by 2009 that number ballooned to over 40 Million [we would now estimate the number to be in the hundreds of millions but no public data exists. There are now governmental initiatives to make the practice commonplace because lawmakers view phone numbers as “important identifiers” and have said “consumers overwhelmingly prefer to keep their numbers. Psychological studies have shown high levels of distress and anxiety when people are without their cell phones, and they now possess similar attachment qualities as teddy bears for youth.

The idea of what is your identity is changing, with technology more and more intertwined into one’s sense of self. When creating an identity protocol, it is therefore important to not only include public identity, but also private identity in the equation.

Non-Standardized Documentation

There are increasing problems with document portability across county, state, provincial, or country lines. Not all identity documents are created equal, and the lack of a global standard is one of the chief concerns of those fighting terrorism, money laundering, drug trafficking, and other illegal activities. Take the U.S. as an example, the problem has gotten so bad that the U.S. government has made it mandatory that residents of Kentucky, Maine, Minnesota, Missouri, Montana, Oklahoma, Pennsylvania, South Carolina, and Washington use a U.S. passport for all domestic travel, because these states do not currently issue a state ID that meets the standards of the REAL ID Act of 2005.

This is not just a problem with centralized identification protocols. Because of a desire of entrepreneurs to create proprietary solutions, rather than open architecture ones, many identity protocols that have or will be proposed on top of distributed databases fall victim to the same problems. It is the view of the Hydrogen developers that tokens or platforms must have the flexibility to read, write, extend, connect, and interact with an identity protocol for it to be most effective. In other words, just adding a public blockchain into the equation does not change fundamental flaws in the approach. Putting a proprietary solution at the protocol level for identity management is similar to the 9 U.S. states that do not meet U.S. identity requirements. There are painstaking changes that will need to be made to create compatibility. This is why Hydrogen is fully committed to a simple and standardized protocol.

Government Blockchain Initiatives

Some of the issues listed above have had the obvious consequences in the public sector, greater interest in blockchain technology. For example, a task force in Illinois presented a plan to create tax records, voting and health histories on a state-run blockchain. The government would become the verifier, rather than the custodian, of people's public service identity, moving from providing data storage to verifying identity. Estonian citizens and e-residents are issued a cryptographically secure digital ID card powered by blockchain infrastructure on the backend, allowing access to various public services, and other countries exploring blockchain ID initiatives include Singapore, Georgia, the UK, and Dubai.

The problem with this is twofold: 1. Governments acting as sole verifiers creates centralization and corruptibility; 2. If every local, state, and national government creates unique private or semi-private blockchains, they will just compound the problems of their non-distributed predecessor databases. For identity management to be truly decentralized and fungible, there must be multiple verifiers and standardized protocols.

Governments may falsely see blockchain “the technology” as a panacea, ignoring the fact that migrating current database infrastructure to a more distributed service is at best only marginally better for the end citizen. At worse, it may make their lives more difficult and complex. Putting false information in an immutable database might be worse than not having any information in there in the first place. Creating systems that are closed architecture and not standardized may compound the current issues seen with global passports and border security.

Introducing Snowflake

To solve the problems mentioned thus far, the team introduces the Hydro Snowflake - unique identity powered by the public blockchain. Why call it Snowflake? They are one of the most beautiful, random, and individualistic things in nature. Not only do scientists believe they come in thirty-five different types, there are differences in the atomic structure of the atoms making up the water molecules, making each Snowflake unique.

Snowflake identities must be “minted.” Each minted Snowflake consists of immutable and non-immutable data, and numerous ways to interact with the data, to be discussed throughout the rest of this paper.

A Tokenized Identity

Every application, web and mobile, requires some form of identification. Users are either stuck repeatedly providing the same information to multiple parties or relying on central parties to relay our information. If those central parties mishandle our info, we are vulnerable to identity theft. All apps must deal with verifying that the information we provide is valid in order to build our IDs for that app.

Thus, each Hydro user has a non-fungible token associated with the wallet (created through the Hydro Raindrop Client-Side) on their phone, which is mapped to their unique HydroID.

This non-fungible token supports storage of three types of data:

- Immutable Data
- Non-Immutable Data
- Metadata
    - Validations
    - Resolvers

Each piece of data associated with a user’s Snowflake can be considered an “attribute” of that Snowflake. When minting or updating their Snowflake, users hash their data with a salt. In cryptography, a salt is random data that is used as an additional input to a one-way function that "hashes" data, a password, or passphrase. The result of this hash is stored on-chain. To the casual observer or would-be attacker, the data is meaningless. However when the user elects to share their plain-text data and salt with a third party, its authenticity is verifiable.

Identity Verification

Validators are third-parties who can make a statement of validation about the data or resolvers tied to your snowflake. In the absence of validators, on-chain data hashes would be meaningless since the hash cannot be reversed.

Off-chain validators can act as parties trusted by individual actors in the decentralized ecosystem. Once the validation happens off-chain, an on-chain record is tied to a user's snowflake. Because nobody can impersonate a validator without access to their private keys, business entities can incorporate on-chain validations into their business logic when querying the blockchain. If a user changes any of the data, it loses its prior validations, and the user would need to acquire new validations for the new data to carry meaning to third-parties.

When the user wants someone to validate their data, they can pass them the plaintext + salt of the data, and the person can hash and compare to what is stored on-chain. If it matches, it would merit a validation.

Validation is conducted off-chain; for instance, DoB validation can be verified by a gov't agency in-person. This validation might carry meaning when proving that you are above a certain age to buy a movie ticket, or when opening a new account at a bank. Alternatively, if a user acquires validations for their email address, they would be able to provide this email to applications without requiring those apps to send a confirmation email, even though the user never publicly announces their email address.

Snowflake Metadata

While immutable and standard data help a user establish a secure and global standard for core identity information, the most powerful aspect of Snowflake is that it allows users to tie an unlimited range of Metadata to their identity by setting third-party dApps as resolvers. As users' interactions with dApps helps build their on-chain identity, they may set a dApp as a resolver for their Snowflake, allowing businesses querying the associated metadata to incorporate it into the logic of their own applications.

Fundamentally, a third-party or dApp validates a certain attribute on a user's Snowflake. An application prescribes meaning to a user based on validations for attributes of their snowflake. Let us more closely examine these meanings in the context of a few examples.

What does validation mean from the perspective of the user? Validations add meaning to a user's core data. Acquiring validations from reputable sources enhances the reputation of a user's Snowflake which can be relied on by applications querying a user's Snowflake.

What does validation mean from the perspective of an app? Validation derives its meaning from off-chain recognition. If an app were to recognize Snowflake as an identity protocol, it could prescribe whatever meaning to validations that suits its needs.

- Example 1, KYC validation: a government could (off-chain) allow users to register their Snowflake for a voting validation. The user could then cast their vote through a third-party dApp such as Horizon State, which would only tally votes from registered Snowflakes. This process would ensure that each person can only vote once, eliminating voter fraud, while providing complete transparency and much greater efficiency to elections.
- Example 2, Social Media: to prevent the creation of fake accounts, an app could implement a system where it links a user's snowflake to their account on the app. Any accounts that have their real name validated by at least x existing users of the app could display a 'verified' checkmark on the UI of the app. Unlike the first example, this example factors validations from individuals instead of from large institutions. Also, this example observes validation for a standard attribute rather than a resolver. Each use-case can recognize validations however works best for it.

What does validation mean from the perspective of the validator? There are many reasons validators may want to attest to various attributes of another person's snowflake.

- Example 1, Social Media Attestation: A person might be participating in a social media app (e.g. LinkedIn) where they want to validate or attest to certain skills of their friends.
- Example 2, State Driver's License: A state or local government may want to validate or attest to the driving skills of a person, in the general interest of public safety. Testing and payment for the identification card can be done off-chain, but every person who observes this user's Snowflake would know that the government government has performed its due diligence.

HYDRO Tokens In Snowflake

Validators must stake in HYDRO tokens to participate in the ecosystem. Tokens are deposited in an on-chain contract tied to their unique address, like a security deposit would be tied to a leaseholder of commercial real estate. Tokens that are removed (or transferred to a third-party) from this contract revoke access of the validator to the ecosystem. At scale, being a validator in HYDRO, and a good actor, will be necessary for all validators globally. If they are not, then any ecosystem for off-chain payments for validations would no longer exist.

This framework ensures that individuals and organizations serving as validators have an interest in validating with integrity and consistency. An application or API querying these validations may define any nature or level of validation they need for the snowflake to be accepted; for instance, they may only grant a user access to certain functions within their application if that user has obtained validation from certain whitelisted or known validators.

As we will discuss later on, Apps, dApps, products, or platforms built on top of the Snowflake can also incorporate HYDRO tokens into their applications. For example, certain kinds of validations or actions may require on-chain HYDRO token transactions, where users would be required to maintain and transfer HYDRO balances.

Open Framework

It is important to note, the proposed framework is just that, an open framework for identity management. Unlike other blockchain products, there will be no centralized decision on the strength or authenticity of attestations or validations, or those who provide them. It will be up to the global community to identify and punish bad actors. We discuss later in this paper potential apps, dApps, and platforms that can be built on top of or integrated into Snowflake to increase the effectiveness of the ecosystem.

Snowflake: Technical Details

There are four entities involved in the Snowflake: users, validators, resolvers, and business entities.

Users

Users mint their snowflakes to represent their identities. They attach data to their snowflake and set resolvers in order to tie any form of metadata to their snowflake. Users can also maintain balances of HYDRO within their snowflake, creating an easy and intuitive mechanism by which a dApp can interact with a user's snowflake. User data is either standard immutable data such Name and Date of Birth, that can only be stored by the owner or approved validator, or non-standard non-immutable data such phone numbers and addresses that can be stored as a string or integer by the owner or by any address approved by the owner.

Validators

A validator is simply a party that attaches itself to a given user's snowflake. Each field in a user's snowflake is tied to a list of validators for that particular field. While anybody who has staked HYDRO can cast validations for any user's snowflake, those validations only carry as much meaning as they have established off-chain. For instance, if a known and trusted KYC party casts a validation on a user's snowflake, a business entity could observe that validation and consider the snowflake to be reliable. Any validation can be stored by any address in an integer format.

Resolvers

While validators attach their validations to a user's snowflake, resolvers are set by the users themselves. Resolvers are dApps that contain metadata about a user. An intuitive example would be if a user set CryptoKitties as a resolver for their snowflake to tie the ownership of certain kitties back to the snowflake address. If that setting were to obtain validations from reputable validators, it would enable them to prove ownership of a certain address that owns CryptoKitties without needing to expose or transact with that address.

Business Entities

Business entities are any applications or dApps that build logic into their applications that rely on information tied to a user's snowflake. For instance, if a user has tied credit-related information to their snowflake through one or several third-party dApps, a business entity might use that metadata in order to determine whether that user would be approved for a certain loan.

Snowflake Smart Contracts

The core snowflake contract stores data, resolvers, and HYDRO balances. It allows users to mint tokens, set fields, and deposit HYDRO. When immutable fields such as Name/DoB are changed, users must mint a new token. When other fields are changed, their resolvers are reset. Resolvers allow users to link their snowflake to external smart contracts which house more data, such as non-binary validations, or if they are an accredited investor. Users, resolvers, or any interested party will be able to deposit HYDRO tokens to the Snowflake smart contract. This will facilitate staking requirements, payments, and other token functionality that will be integrated seamlessly into the Hydro ecosystem as it develops.

3rd party dApps:

- Hydrogen will create the initial core Snowflake data validation dApp which is a “gateway” to compliant third-party dApps (we will have guidelines about how these apps should look)
- Hydrogen will create logic for dApps to allow sending, staking, and fees in Hydro
- All dApps would want users to set their contract address as a resolver

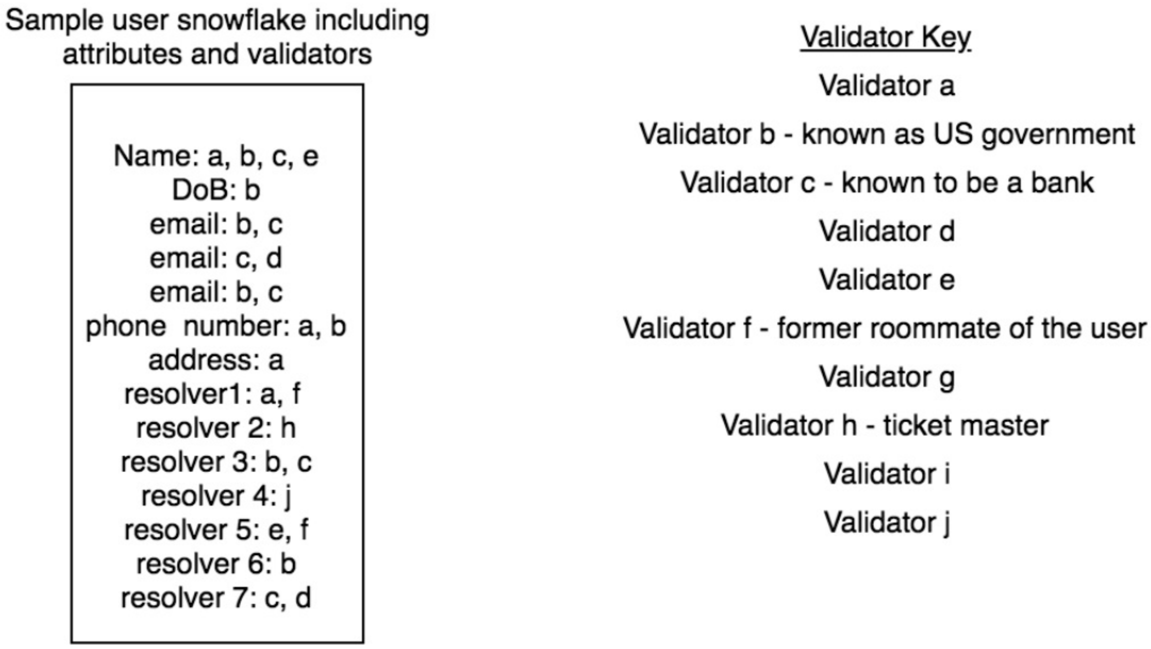
The Base snowflake identity consists of the summation of:

- Standard fields that are immutable on-chain and can be minted once by the owner
  - Full Name
  - Date of Birth
- Standard fields, can be added and voided by the owner
  - Name prefix/suffix
  - Emails

- Phone numbers
- Addresses

- Resolvers - can be added by token owners or if given allowance by the contract owner
  - Ethereum smart contract addresses
- Validation - any address with a HydroID can validate any attribute for any snowflake as long as they pay the gas costs.

A user’s Snowflake acts as an anchor point for data from all that user’s dApp interactions. A third-party app can see who validated which fields for the user. For example, in the image below, resolver 1 may be a social review dApp to show that the user has been validated as a good roommate. A business entity can see that validator f, a former roommate, validated the owner's info. It can therefore, in its business logic, allow reviewers from resolver 1 to write a review on the UI of its platform because their reviews apply to this snowflake owner.



Sample user snowflake including attributes and validators

Name: a, b, c, e
DoB: b
email: b, c
email: c, d
email: b, c
phone number: a, b
address: a
resolver1: a, f
resolver 2: h
resolver 3: b, c
resolver 4: j
resolver 5: e, f
resolver 6: b
resolver 7: c, d

Validator Key
Validator a
Validator b - known as US government
Validator c - known to be a bank
Validator d
Validator e
Validator f - former roommate of the user
Validator g
Validator h - ticket master
Validator i
Validator j

Snowflake API and Hydro Mobile App

Hydrogen’s Hydro API will facilitate user and business entity interactions with Snowflake smart contracts. The API provides end users the ability to register their HydroIDs, a prerequisite to minting their Snowflakes, through the Raindrop API integration into the Hydro mobile app. In the next iteration, users will be able to mint their own Snowflake associated with their HydroID through the Hydro mobile app while the Hydro API handles the direct interaction with the blockchain. The UI on their mobile app will allow them to observe validations they have obtained from addresses whitelisted by the Hydro API. They will also be able to set resolvers through their Hydro mobile app to attach a broader range of metadata to their snowflake.

Business entities will be able to use the Hydro API to query the Ethereum blockchain for information contained within the Hydro ecosystem. The API will provide on-chain information to applications in a digestible format that can be easily encoded into their business logic without requiring them to have blockchain developers.

Mirroring The ERC-721 Contract Standard

ERC-20 tokens, such as HYDRO, share the characteristic of fungibility, meaning each token is seamlessly and equally interchangeable with any other. This makes sense for tokens in the ERC-20 standard since each token has the same functionality as any other token. For an identity protocol, however, non-fungibility drives the meaningfulness behind ownership. If we were able to swap our identities out amongst ourselves with no difference, those identities would carry no value to any observer. Ethereum Request for Comments 721, or ERC-721, is an Ethereum proposal introduced by Dieter Shirley in 2017. Although HYDRO the token itself is built on the ERC-20 standard, our Snowflake protocol's smart contracts more closely mirror the dynamics found in ERC-721 tokens. These are known as “non-fungible” tokens.

The non-fungibility of each Snowflake is crucial to allowing users to prove ownership of the information associated with their identity. The value of the Snowflake identity is not that it can be exchanged for some monetary value, but because it has unique characteristics that build a user's on-chain identity. With this in mind, we have moved slightly away from the ERC-721 standard to disallow transfer of ownership of an identity.

A persistent concern in open-source and blockchain communities is the fragmentation of developer effort across multiple projects and standards. We are very aware of this risk, and have designed Snowflake in such a way as to make this eventuality as unlikely as possible. Our break from ERC-721 should not be taken as a criticism of this work, but rather a reflection of the simple reality that identities are anchored to their owners in a way that other unique and collectible tokens are not. Within this constraint, Snowflake was designed to be fundamentally modular and open; it can flexibly incorporate a wide variety of use cases and will serve as a common protocol for making identity-related claims.

Implications for Financial Services

The open framework of Snowflake will make products, platforms, apps, and dApps built on top of the protocol integral to its long-term success. Below we examine some initial applications that the Hydro community will champion:

Universal Account Onboarding

Through integration with global KYC providers as validators, Hydro can create a standard one-touch digital account onboarding standard that can adapt to the wide range of KYC standards existent in today’s world.

Validator Rating System

This simple dApp would create an upvoting/downvoting system for validators across multiple identity areas. A reputation-based scoring system would create incentive-driven honesty in votes. This decentralized reputation-building can prescribe greater meaning to some validators than a binary process.

Machine Learning Validation Standard

The Hydrogen platform contains the Ion AutoML API. With sufficient validations globally, a product can be created using the AutoML API that rates, sorts, ranks, flags, and removes validations and validators in a decentralized and data driven way. Smart contracts can be integrated on top of the AutoML capabilities for transparency.

Document & Contract Verification Standard

The next phase of Project Hydro is called Ice. This is a document management protocol. The Snowflake, combined with Raindrop, will be integral for the scaling of Ice. A large problem with e-signing technologies is there is never any authentication or verification done, other than single factor usernames and passwords. Validated snowflakes and multi-factor authentications for any document signings or contract sealing can be built into the Hydro mobile app. Some simple dApps built on top of the Ice protocol can also integrate popular e-signing softwares such as DocuSign and Adobe Sign.

Payment Verification Standard

An upcoming phase of Project Hydro is called Tide. This is a payment and data privacy protocol. There is great opportunity to create a dApp that can reference validations and create “Levels” or strength of the validation. An implication of this might be a plug-in for financial services websites that checks the level of validation. A highest level validation may require no extra verification or authentication, while the lowest validation may require a secondary form of ID.

Anti-Fraud POS dApps

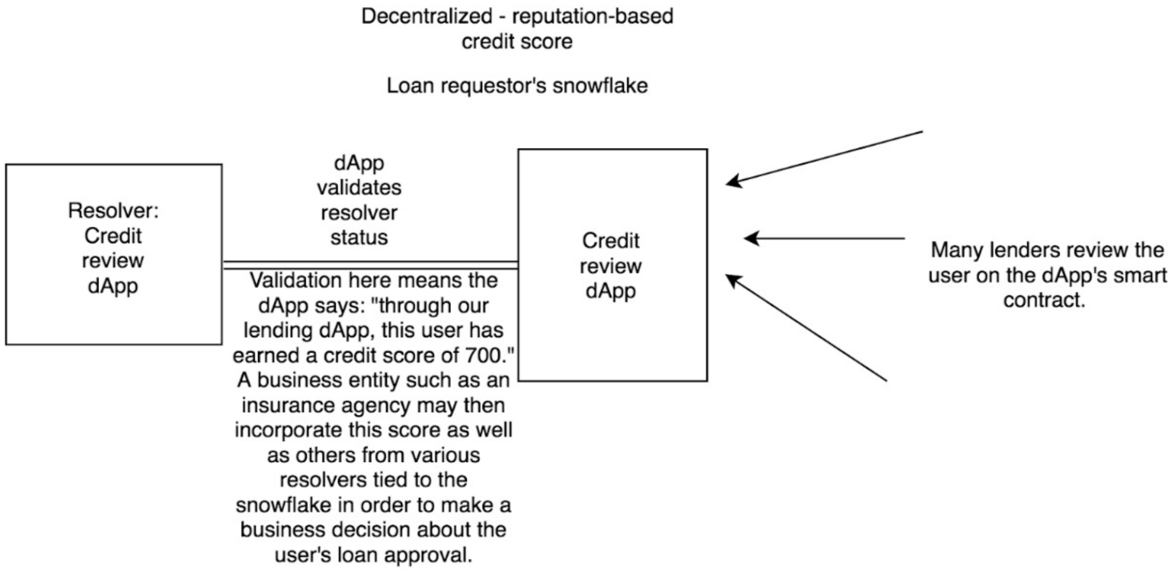
Most point of sales systems require simple swiping or chip verifications on debit and credit cards. There are no additional identity checks done during the sale, only post-sale, as examined in this paper. As firms like Square, Paypal, Braintree, and Stripe increase their presences globally, billions will have access to instant point of sale transaction protocols.

There are very interesting dApps that can be built that integrate the Snowflake, Raindrop, Tide, and Mist phases of Hydro to produce a decentralized POS network.

Global Credit Scoring

Access to credit is a huge global problem, and one of the major issues affecting the 2 Billion unbanked. To counter this problem, there has been a FICO scoring system setup in the U.S. to attempt to use financial data to validate credit worthiness. But this system is fundamentally flawed in that it takes in no “social proof” and only accounts for those already in the financial system with bank accounts and credit cards. The Hydro API can provide business entities with the information they need to build more robust credit scoring models without relying on central parties to store sensitive user data.

A third-party business entity can rely on information tied to a user’s snowflake through a resolver for that user’s credit scoring data in order to drive its business decision in delivering a loan.


Decentralized - reputation-based credit score
Loan requestor's snowflake
Resolver: Credit review dApp
dApp validates resolver status
Validation here means the dApp says: "through our lending dApp, this user has earned a credit score of 700." A business entity such as an insurance agency may then incorporate this score as well as others from various resolvers tied to the snowflake in order to make a business decision about the user's loan approval.
Credit review dApp
Many lenders review the user on the dApp's smart contract.

Risks

The Snowflake ecosystem is dependent on off-chain validators as best actors, and a global decentralized community that would punish bad behavior. For example, we do not want to encourage the same “black markets” for verification and documentation that exist off-chain and bring them on-chain, so it is imperative that the ecosystem function as designed. This is why the HYDRO token and staking are so vital to keeping the ecosystem honest.

There is additional risk of “fragmentation” within the ecosystem. It will be up to a business or website to decide how much validation or attestation is acceptable to approve a user. Because Snowflake is a protocol, and not a product, it will be imperative that best use cases are standardized quickly to prevent this fragmentation of acceptance. For example, a validated state driver's license may be accepted on Amazon for checkout, but on Google there might be an additional social attestation required. It is the Hydro team's goal to provide best practices, sample apps, and widgets for sites to use for various use cases to combat this issue.

There is an "educational" risk to the ecosystem as well. Many incumbent blockchain identity ecosystems are built in a closed architecture or private way. There has been a huge disinformation campaign from private blockchain providers on the perceived weaknesses in public blockchain. The Snowflake ecosystem is dependent on users trusting the encryption on the public blockchain and their smartphone.

Conclusion

Identity management globally is broken and it is only getting worse as we approach the dawn of the Web 3.0. Identity remains centralized, prone to corruption and theft, and billions are still shut out from financial services solutions in part because of it.

The Hydro Snowflake framework is being implemented to solve key parts of the identity management problem:

- Creation of a standard decentralized framework to store personal information that can be encrypted on-chain
- Creation of an off-chain validation and attestation network that links to on-chain data
- Creation of standardized apps, QR codes, UI widgets, and other products on top of the Snowflake protocol that can be easily integrated

The Hydro team believes the framework set forth can be the standard identity management protocol of the Web 3.0. Due to the ease of use of the Hydro API both apps and dApps can quickly implement the Snowflake architecture into their own.

Sources

PNAS.org - http://www.pnas.org/content/110/32/13216

Social Security Administration - https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html

History Channel - https://www.history.com/news/the-history-of-birth-certificates-is-shorter-than-you-might-think

Ancentry.com - https://blogs.ancestry.com/cm/what-can-your-surname-tell-you/

CNN.com - https://www.cnn.com/2013/01/18/justice/florida-cuban-birth-certificates/index.html

Watchdog.org - https://www.watchdog.org/florida/those-with-fake-birth-certificates-find-it-s-easy-to/article_a3935cbf-74b8-5237-9b0a-ae17748f6786.html

Martin Private Investigators - http://www.martinpi.com/your-cell-phone-number-is-your-new-social-security-number/

Statista - https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/;
https://www.statista.com/statistics/188511/mobile-to-mobile-telephone-numbers-in-us-porting-database-since-2003/

Federal Register - https://www.federalregister.gov/documents/2017/11/27/2017-25458/nationwide-number-portability-numbering-policies-for-modern-communications

Psychology Today - https://www.psychologytoday.com/us/blog/fulfillment-any-age/201609/is-why-we-cant-put-down-our-phones)

Symantec - https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Chargebacks911 - https://chargebacks911.com/chargeback-stats-2017/

Travel & Leisure - http://www.travelandleisure.com/airlines-airports/no-drivers-license-tsa-rule

Coindesk - https://www.coindesk.com/illinois-eyes-blockchain-for-ids-and-public-asset-management

Enterprise Innovation - https://www.enterpriseinnovation.net/article/how-are-governments-using-blockchain-technology-1122807855

W3.org - https://www.w3.org/DesignIssues/Metadata.html

PSU Meteorology - http://news.psu.edu/story/141325/2009/02/18/research/probing-question-each-snowflake-really-unique

Wikipedia Cryptography - https://en.wikipedia.org/wiki/Salt_(cryptography)