Using Blockchain-Based Digital Identity and Verifiable Credentials for Chess

Author
Bruno Martins
Principal Architect, Algorand Foundation

Contributors
World Chess (LSE:CHSS), GM Evgenij Miroshnichenko

Abstract

A globally beloved and ever-challenging game, chess also has a notable history as a proving ground for new technologies. One immediately recalls the famous Deep Blue vs Kasparov matches, which broadly changed the perception of AI and machine learning. With this paper, we present the chess community with another opportunity to demonstrate what is possible with cutting-edge technology – all while improving the user experience of the chess ecosystem in the process.

This document conceptualizes a new system that utilizes blockchain to establish secure, portable digital identities and verifiable credentials[1] for chess players everywhere. Utilizing standardized data models and decentralized identifiers (DID)[2], the proposed system is secure and privacy-preserving. If adopted, it will allow chess players to independently manage their identity and credentials across chess platforms and organizations. This means that players could port their identity, achievements, records of play, rankings, and rewards across not only various online chess platforms, but seamlessly from the digital world to in-person games and tournaments. For chess organizations, it means simpler verification of player identities and records, a new tool for maintaining integrity across both online and offline tournaments, a simple solution for transparently adjusting player ratings across various federations, and more.

The system – conceptualized by software architects at the Algorand Foundation with contributions and counsel from leaders at World Chess (operators of the FIDE Online Arena) and others – will bring efficiency to chess entities and organizations, and a simpler, more streamlined experience for chess players, all without sacrificing security or trust. It will break down siloes between platforms, creating a more connected and inviting chess ecosystem for all.

Contents

1. Introduction

In today's chess ecosystem, composed of international and national chess federations, formal chess clubs, and online chess platforms, players must create a new account, using, at least, an email address or preferred username, everywhere they'd like to play. This means establishing a distinct identity with each entity, which results in a players' history, achievements, and rewards being locked within isolated platforms, neither portable to nor verifiable by other organizations. Furthermore, these accounts are not typically linked to a player's real-world identity, meaning there is no Know Your Customer (KYC)[3] process to confirm that a user registering an account under a given name is indeed the real-world person they claim to be. (Certainly none that is universal and portable between entities.)

In today's environment, where billions of chess games and tournaments occur online each year, it is remarkable to realize that players' online achievements and rewards are not easily portable to in-person tournaments. With no standard system in place, it is cumbersome and time-consuming for entities to verifiably connect an online player's identity to that of a real person – oftentimes taking several hours or more.

In short, for the vast majority of chess players, the ecosystem that exists today is, in fact, barely an ecosystem at all, but rather a side-by-side collective of walled gardens.

In the system we propose, a player's identity – including a record of good or bad standing, FIDE titles[4], etc. – could be standardized for verification, with trust anchored in the issuing organization – such as World Chess, FIDE, US Chess Federation, and so on. This would allow players to move freely between platforms and the tournament systems of various organizing bodies, and create a more efficient system for these entities to track and engage with chess players globally.

Decentralized Identifiers & Verifiable Credentials

Our proposal is based on decentralized identifiers (DIDs) and verifiable credentials (VCs), two established solutions in the decentralized technology sector. DIDs are unique, user-controlled identifiers that enable a person to be verified without reliance on a central authority. (They are sometimes referred to as "self-sovereign identity," given that control of the identifier sits with the individual.) DIDs are cryptographically verified and built on distributed networks, helping ensure their security. The Decentralized Identity Foundation (DIF) and W3C[7] are two bodies that develop open-source, standards-based design implementations for DIDs, while the OpenWallet Foundation[6] develops open-source implementations and promotes interoperable multi-purpose wallet solutions that anyone can use in building similar solutions.

VCs are essentially digital documents that attest a user's identity or other credentials. They can prove a user's education level, work history, or in our case, for example, a person's official chess rating. VCs have been standardized by the World Wide Web Consortium (W3C), among other recognized bodies.

Both DIDs and VCs already exist with proven designs for implementation. Our proposal takes these technologies and applies them to the chess ecosystem, envisioning a system that brings efficiency and interconnectedness to chess platforms and governing organizations, and creates a seamless, empowered experience for chess players.

It is worth noting that this problem of "walled identity gardens" is not unique to chess, or even to the broader world of online/offline gaming. Many other domains–such as education, employment, and healthcare–face similar challenges. The same specifications utilized in our proposal for chess can also provide potential solutions to these challenges.

2. Objectives

Our proposed solution aims to enable the following for players and entities across online, in-person, and hybrid chess environments.

> **/ Establish a unified solution for verified, portable chess player identities:** Our solution enables chess entities to issue a trusted, verifiable identifier to players that is recognized and transferable to all other participating chess entities. Serving as a type of "**universal chess passport**," a DID can uniquely bridge online platforms and offline tournaments. It creates a unified, verifiable record of a player's accomplishments, rankings, and history across all chess mediums. Where relevant, entities may also request players complete a formal, third-party verified KYC process; this could be a one-time process, accepted by all participating chess organizations and apps. Other VCs issued to a player and connected to their digital identity could be used for player titles (ie "Grandmaster," or "International Master"), proof of participation or result in on- and offline tournaments, record of good standing, accrued rewards, etc.

Verifiable Credentials are stored in the players own wallet and establish a permanent, verifiable record of a player's achievements and chess career history. With customizable privacy controls, this data can be selectively shared and integrated into chess communities, improving recognition of long-term contributions to the game.

> **/ Skills verification for coaching and content creation:** Another use case for VCs in chess includes formal recognition of a chess coach's credentials, or a content creator's expertise. Students and fans can then make better-informed decisions about the resources and training opportunities they seek.
>
> **/ Lifetime achievements & history:** VCs, anchored in a decentralized system, establish a permanent, verifiable record of a player's achievements and career history. With customizable privacy controls, this data can be selectively shared and integrated into chess communities, improving recognition for players' long-term contributions to the game.

/ Bolster rating transparency and transferability: VCs create a tamper-resistant record of a player's rating across national federations, making it easier for them to move between different rating systems (e.g., FIDE, USCF) and have their rating changes accurately reflected. Effectively this creates an interoperable system where a chess player simply has to show up – or log on – connect their wallet, and start playing. This vastly streamlines the verification process for tournament organizers, reducing administrative overhead while bolstering trust in participants. By removing the time-consuming and document-laden burden of current tournament registration and rating verification processes, organizers can also more easily attract stronger players to their events.

/ Enable cheat detection and encourage fair play: Integrating DID with VCs allows a player's history and reputation to be verified across platforms. If a player is banned for cheating on one platform, their credentials can be revoked in a transparent manner. This enables each chess entity to independently make decisions regarding a player's ability to participate on their platform – and to cross-check a player's record on other platforms as well, to help guide decisionmaking. Digital records of a player's tournament participation and fair play history reduce paperwork for organizations while maintaining tournament integrity. Because DID enables seamless portability of players' identities and associated records, players can maintain consistent credibility across the entire chess ecosystem.

> **/** When a credential is revoked (e.g., for cheating), the system should ensure due process, establishing appeal mechanisms so players can contest incorrect reputation changes, with transparent criteria for credential reinstatement.

/ Improve tournament registration and prize distribution efficiency: Tournament organizers can use verifiable credentials to confirm a player's eligibility and identity (e.g., age, nationality, rating, blockchain/ledger addresses, payout methods) without handling sensitive documentation. DIDs will also simplify the registration process by automatically confirming details like rating, titles, or membership in a federation, reducing the time-intensive administrative burden (often taking several hours or more for major open tournaments) – for both player and organizing entity. This can apply to tournaments at all levels, but may be especially useful in lower-tier tournaments (ex. university teams, junior clubs), where lack of proper verification controls – and sometimes, lack of government IDs or paperwork for young players – can lead to fraud, such as one player competing under another's name.

Further, smart contracts built on-chain can automate payouts instantly based on verified tournament results and identity. In the current environment, where phishing and scam attempts are increasingly common around tournament prize fund distribution, being able to instantly verify a player's identity can minimize fraud risk. Integrating a self-custodial, on-chain wallet solution also opens up the possibility of a tournament organizer distributing prize funds directly to a user's wallet as stablecoin or other token.

/ Reward players for their achievements and enable greater flexibility for reward redemption: Chess is a competitive game, with many people playing for the potential of rewards, whether monetary, points-based, or otherwise. In our system, where rewards can be directly and instantly delivered to a verified user's wallet, there is the expanded potential for rewards to be portable across platforms as well. In one simple example, a user could accrue a certain threshold of rewards points via one online chess platform, then connect their wallet at an in-person tournament reserved for high-volume players, redeeming those points for access to play. Because everything is attached to the user's DID, verification and movement of rewards is seamless. In another example, a user could play chess actively on platform A, then redeem their accrued points on platform B to unlock an exclusive live session with a GM or other access other ratings-gated content. This would encourage players to more readily explore the offerings and unique benefits of platforms across the ecosystem.

3. Acknowledgements & invitation to collaborate

This proposal was developed by software architects at the Algorand Foundation, in close partnership with World Chess, operators of the FIDE Online Arena. Particular thanks to World Chess COO, Matvey Shekhovtsov, and chess grandmaster Evgenij Miroshnichenko, both of whom contributed essential insights and guidance throughout the paper's development. Thanks also to Kim Hamilton Duffy, Executive Director at the Decentralized Identity Foundation[5], for reviewing the proposal and providing valuable feedback.

The system described in this paper is currently in development on a small scale to test its feasibility. We invite chess platforms, organizations, and players to collaborate in its further development.

4. Proposed solution design

4a Components and definitions

/ Self-custody wallets: Self-custody wallets have been popularized along with the rise in blockchain and cryptocurrency adoption, but their use extends far beyond Web3. The main idea to understand is that the user is the only one who has control over the private keys that control the assets in the wallet. This is in contrast to how most applications work today, where a user has to trust the platform to keep their assets safe. In our proposal, the idea is that the chess player, not the chess platforms or organizations, has control of the keys that are linked to their identity and associated credentials.

/ Decentralized identifiers (DIDs): Today, when we "sign up" or register with a platform, we are given an identifier – a username or an alias – that is unique to that platform. All data that is associated with that identifier is stored in the platform's database, and the user has no control over it, including no direct ability to delete their data or take it with them to another platform. DIDs are a new type of identifier that are global, controlled by the user and span across industries and platforms. These identifiers are fully under the control of the DID subject (in our case, the chess player), independent from any centralized registry, identity provider, or certificate authority (in our case, a chess federation or online gaming portal). DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID documents that contain cryptographic material and other metadata.

/ DID aliases: DIDs are a technical standard that participating platforms and organizations would use to identify a player. In all likelihood, however, each platform and wallets would still choose to present players with an alias, or username, unique to their platform. The formal identifier attached to the alias would now be controlled by the player, however, rather than controlled by the organization.

/ Verifiable credentials (VCs): Verifiable Credentials are a standard for expressing credentials in a way that is cryptographically secure, privacy-respecting, and machine-verifiable. VCs can represent statements made by an issuer about a subject, such as a player's identity, achievements, rewards and good standing.

/ Verifiable data registry: In a decentralized system, there is, of course, no central authority that is alone empowered to attest to a user's identity or credentials. So a common data registry is needed where metadata information, or proofs, can be stored and accessed by system participants in order to be verified. This data registry does not need to live on an open, public blockchain or distributed ledger, although by doing so adds critical benefits to the system. These include transparency and accessibility without controls (meaning all entities involved can view and add data), no single actor owns the registry (meaning no single chess entity could change data about a player in a secretive or preferential way), and any history of changes are easily tracked and audited.

/ Passkeys: Passkeys are an authentication mechanism growing in popularity across the digital world. A passkey, using public-private key pairs, saves users the hassle of remembering passwords for websites or apps, and instead relies on the user's possession of a device, such as a smartphone or computer, to authenticate the connection (i.e., to login) using either biometric data or asking a challenge prompt. In practice: the app you are attempting to login to sends a challenge to your device, either asking for your fingerprint, face scan, or an authenticator code. Once you complete the challenge, you are logged in. No need to remember or enter a typed password.

/ Issuer: In the industry-standard model for a DID and VC system, an "issuer" is an entity that makes a claim about a subject in the form of a verifiable credential. In the context of chess, the issuer could be a chess platform, such as World Chess, Chess.com, Lichess, FIDE, etc. Any organisation that can make a claim about a player.

/ Holder: In the industry-standard model for a DID and VC system, a "holder" is an entity that holds a verifiable credential. In our case, most often the holder will be the individual chess player, but it could also be an organization or platform.

/ Verifier: In the industry-standard model for a DID and VC system, a "verifier" is an entity that verifies a verifiable credential. In our case, the verifier could be a chess platform or a tournament organizer, etc.

4b Technical standards utilized

/ Issuer, holder, and verifier in a Verifiable Credentials system
The following diagram is a generalized example of how an Issuer, Holder, and Verifier compose a system for the issuance and management of Verifiable Credentials.

Adapted from source: decentralized-id.com

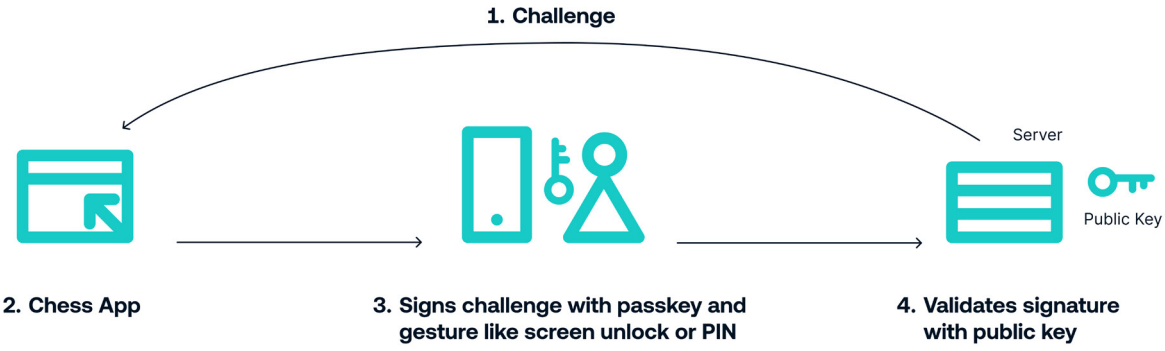
/ Authentication and Authorization

While self-custody wallets have largely gained popularity in blockchain and cryptocurrency use cases to this point, they can be used for many different purposes, such as connecting a user to a platform or application. We propose here that chess players use self-custody wallets to securely connect with all chess entities.

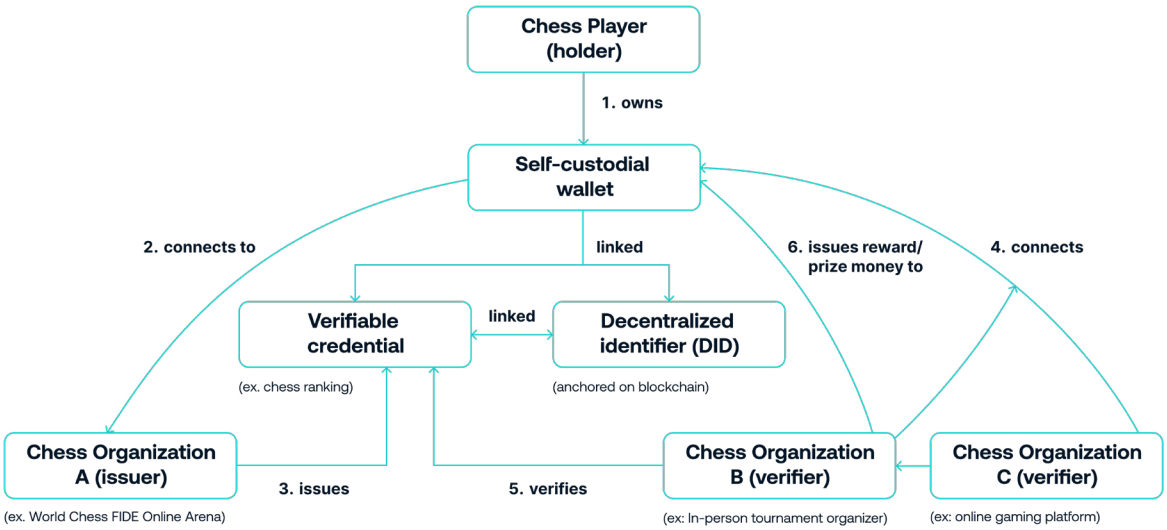
Utilizing known technologies including self-custody wallets and passkeys, the user experience for authentication and authorization across platforms can be as simple for a user as scanning a QR code with their wallet app.

Unlike passkeys approaches you see on Google Chrome or within Apple's iCloud Keychain, in this system a user's keys are stored in their wallet, and not in the platform or in the cloud. The user is the only one that has control over the keys that are used to authenticate and authorize themselves to the platform.

Here is a generalized diagram of the passkeys authentication flow:



4c Conceptual system architecture



4d Use case examples

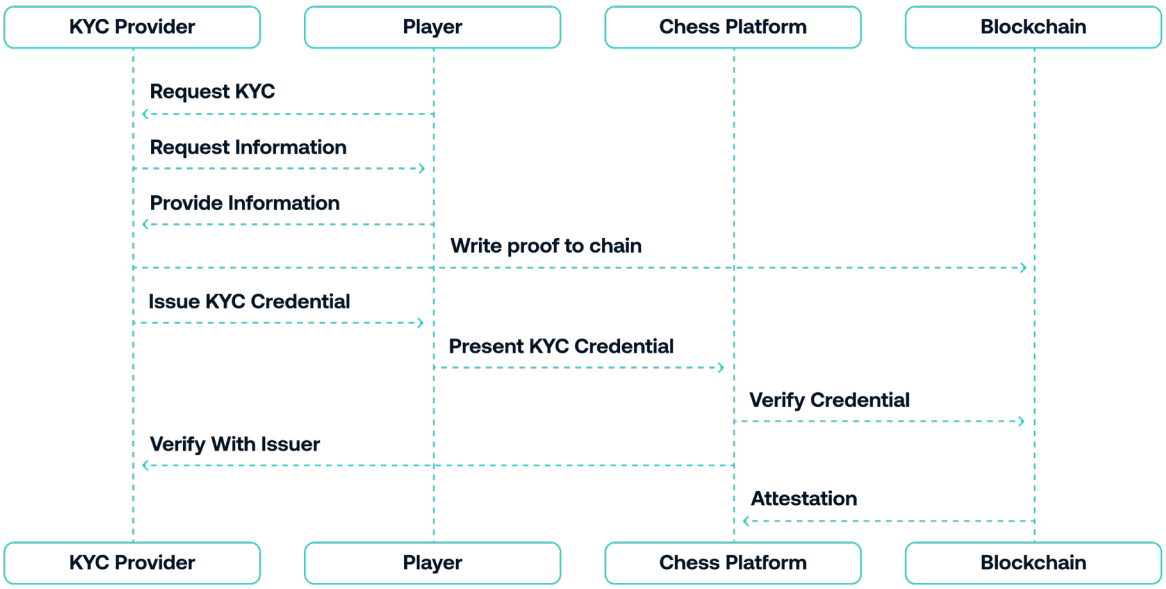
/ KYC checks & reusability

Although not a hard requirement for all chess platforms, there are scenarios where it will be necessary to link a player's alias or username to a real person. This can be useful for facilitating tournament payouts or in-person registrations, or even to disincentivize cheating.

In this model, the KYC-related VC is issued by a third party specializing in this type of verification (the "KYC Provider").

Once a KYC VC is issued, the player can use it across all chess platforms and organizations that require KYC checks. The VC can be presented through a web platform, wallet-to-wallet communication, or even via a QR code.

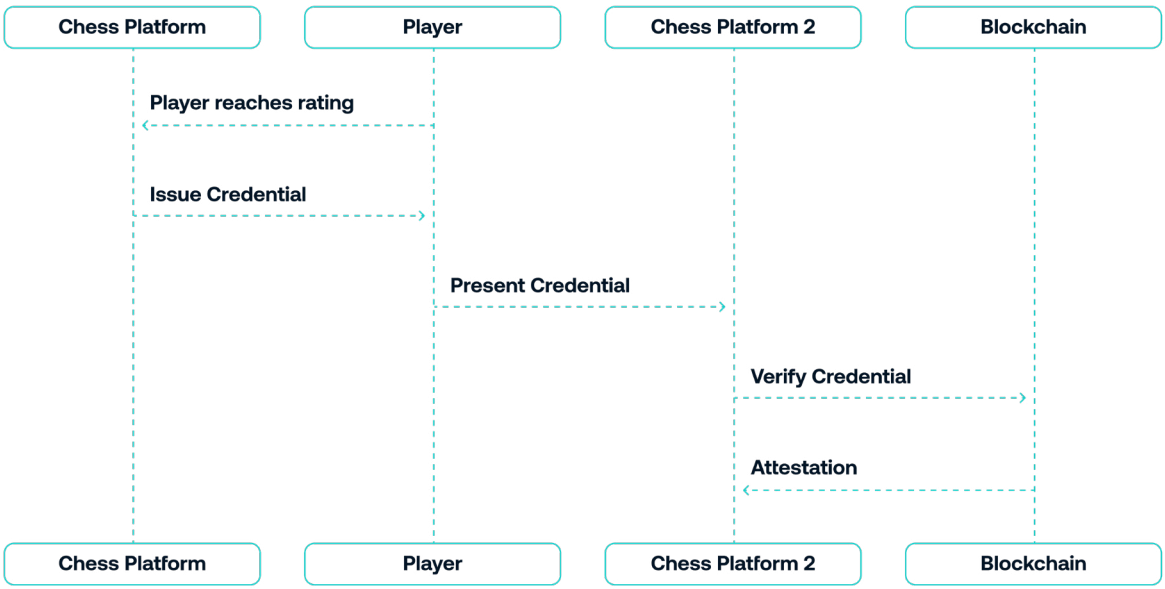
Another variant of this use case could have the chess platform itself acting as issuer of the KYC credential.



/ Achievements and rewards

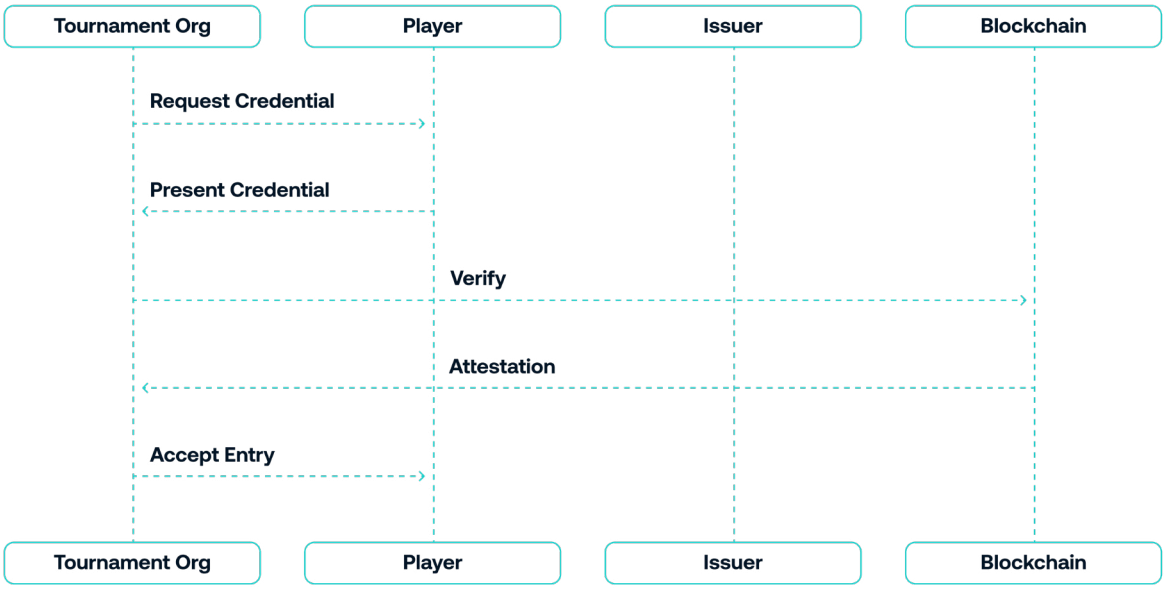
Players can earn achievements and rewards on different chess platforms. For example, on the FIDE Online Arena operated by World Chess, players compete for official ratings and titles and can participate in online tournaments with significant payouts or other valuable prizes. These achievements and rewards, however, are usually locked within the platform and cannot be ported to other virtual chess platforms, or to most in-person games and tournaments.

With our proposed system, players would receive VCs to represent their achievements and rewards. These can be, for example, proof of winning a tournament, achieving a certain rating, or even a good conduct badge. Imagine a player competes in a virtual tournament on platform A, and achieves a certain rating. Platform A could issue the player a VC, stored in the player's wallet, to mark this rating. The player could then connect their wallet to platform B, platform B could confirm the rating they've earned on platform A, and the player could then start playing on platform B at their verified level. All simply and seamlessly by connecting their wallet to the given platforms.



/ In-person tournaments

Organizers of in-person chess tournaments may want to welcome highly-ranked online chess players, but would require players to prove who they are and what they've achieved – a process that today can take several hours or more due to the volume of players, need for various ID documents like passports and drivers licenses, and even transliteration rules. In our scenario, a tournament organizer could request the player connect their wallet (via QR code scan, etc.) to verify their DID credential (even being a KYC-issued VC, if required). With the player's digital identity connected to their real identity, verifiable by the tournament organizer in real-time, the organization could seamlessly accept the player into the tournament.



4e System principles

All implementations and designs outlined in this paper uphold the following principles:

/ Portability: A user (chess player) should be able to take their identity, credentials, and digital assets (such as accrued platform rewards) to different chess platforms and organizations.

VCs can be issued by one platform and verified by another, allowing players to carry their achievements, ratings, and rewards across different chess platforms and organizations. An example would be a player that has achieved a certain rating on one platform and proven their good standing, could use that same credential to register on another platform and begin playing at a given ranking, without having to rebuild their record from scratch.

/ Digital identity-centric, linkable to real identity: The entirety of this proposal is anchored on the idea that a user's DID is portable across various chess platforms (and, in theory, to the rest of the digital world as well.)

A user could decide to have multiple DIDs, and choose which one to use for different purposes. The system should allow for the player to choose one of their DIDs to link to their real identity through a KYC process, resulting in a VC. This would enable the player to prove who they are online and prove their identity at in-person games and tournaments. It also, however, unlocks other potential use cases such as authenticated statements or valid signed documents.

/ Abstract technical complexity for users: Most Web3 applications are built on top of blockchain technology, which is complex and hard to understand for the average user. Traditionally the user would have to know what an address is, a private key, transactions, transaction fees, etc. Our proposed system for chess is designed to reduce all complexity for users down to a single piece of information that they would need to be responsible for – the 24-word seed phrase, used to backup and recover their wallet's keys (and with the keys, access to their assets, identifiers and credentials).

/ No fees for onboarding: Onboarding a user to this new system–that is, creating the user's DID– will require some kind of transaction. In most Web3 scenarios, the user would need to have or purchase cryptocurrency to pay for the associated transaction fees. We propose that either the wallet provider or the DID-issuing platform be responsible for paying user transaction fees during onboarding. Some blockchain networks–such as Algorand, on which we are developing the initial system implementation– have native properties that allow for the delegation of fees. Algorand natively supports grouping transactions together by multiple parties and pooling the fees. If this system were implemented on other blockchain networks, alternative methods should be applied to enable wallet providers or issuers to pay for user onboarding fees.

/ Storage and recovery of DIDs: The player's digital identifiers, and the private keys associated with them, should only be available within the wallet. In case a player loses their device or wallet, their identity and related keys should be recovered by entering a 24-word seed phrase, similar to how most web3 wallets work today. This 24-word phrase (sometimes also called a mnemonic phrase or recovery phrase) is like a master key for a user's account(s). It is a randomized selection of 24 words. Anyone who gains access to another user's seed phrase could, in theory, access the related accounts, and the identifiers, credentials, or funds within it. In our proposal, all a user needs to remember is this private 24-word phrase.

/ Peer-to-peer (P2P) communication: Many of today's Web3 applications rely on an intermediary, frequently a private, centralized company named WalletConnect, to connect a user's wallet with other applications or platforms. In our opinion, this is one of the elements of Web3 that has prevented its more widespread adoption, as it adds friction and complexity for users, and signals a lack of maturity to the rest of the digital world. Instead, we believe that the user's wallet should be able to communicate directly with a given platform or application, without the need of an intermediary. A combination of existing open-source protocols and standards make this readily possible.

/ Privacy by design: A user's wallet should hold the user's data, digital asset information, identity, and credentials, and only the user should be able to control what information is shared with a platform or organization. Also, In this system, different contexts require varying levels of privacy protection. For casual players, complete anonymity may be preferred; coaches might require credentials demonstrating verified expertise without revealing personal details. The system must allow participants to share the appropriate details depending on context.

/ Revocation and transparency: VCs can be revoked by the issuer, and the status of a user's credentials can be checked at any time by any other verifier in the system. This allows platforms to revoke a player's achievements, rewards, or good standing if they are found to be cheating or violating the platform's terms of service. This way, a user's actions in one platform can have consequences in another.

/ Privacy-preserving: Some user information may be sensitive, such as KYC data or real identity information. Tools like Zero Knowledge Proofs or selective disclosure techniques should be used where possible so that users need only to share necessary information when presenting their credentials to new entities or platforms.

> / Blockchain's immutability creates tension with privacy regulations like GDPR's 'right to be forgotten.' The system addresses this by storing personal information off-chain.

5. Conclusion

The proposed system is designed to be decentralized, secure, and privacy-preserving. It utilizes accepted standards for digital identity and verifiable credentials to enable chess players to manage their identity and credentials – and to port their achievements, rewards, and more – across a myriad of formerly isolated chess platforms and organizations.

6. References

[1] W3C. (2019). Verifiable Credentials Data Model 1.0. Retrieved from https://www.w3.org/TR/ vc-data-model/
[2] W3C. (2021). Decentralized Identifiers (DIDs) v1.0. Retrieved from https://www.w3.org/TR/ did-core/
[3] Wikipedia. (n.d.). Know your customer. Retrieved from https://en.wikipedia.org/wiki/ Know_your_customer
[4] Wikipedia. (n.d.). FIDE titles. Retrieved from https://en.wikipedia.org/wiki/FIDE_titles
[5] Decentralized Identity Foundation. (n.d.). Retrieved from https://identity.foundation/
[6] OpenWallet Foundation. (n.d.). Retrieved from https://openwallet.foundation/
[7] World Wide Web Consortium (W3C). (n.d.). Retrieved from https://www.w3.org/