A Privacy-Preserving Distributed Identity Offline-First PoCP Blockchain Paradigm

Andrew M. K. Nassief
The Lonero Foundation
andrew@etherstone.org

BitBadges is a privacy preserving distributed identity platform that plans on utilizing CouchDB, the decentralized-internet SDK by Lonero, Blake3 hashing, and a PoCP or Proof of Computation consensus algorithm. It is privacy-preserving and offers a unique proposition for traditional blockchains centered around consensus algorithms. This paper introduces the conceptual design for BitBadges in its second version and as its own blockchain platform and cryptocurrency. The aim is to introduce various researchers to distributed consensus through an identity-based platform, while still keeping its decentralized and privacy-preserving nature. The main distributed computing paradigm or architectural design is centered around Peer to Peer Client Server models and a Point to Point message model. Its distributed system is centered around a grid computing design based off of fault tolerance and censorship-resistance. It also implements lockstep and modular operations. BitBadges was first iterated as a NFT hashing/badge creation solution and has slowly transitioned to an alternative to ERC721 to its own blockchain. BitBadges will be interoperable with various sidechain integrations for badge issuing and identity measures. These are further intentional integrations to make BitBadges further decentralized. The aim is to create a new model for distributed identity centered around PoCP.

1.0 Introduction

Traditional consensus algorithms such as PoW and PoS have certain vulnerabilities. PoW consensus such as what is found in Bitcoin, is vulnerable to double-spending or 51% attacks [1]. PoS Consensus isn't censorship resistant and not always fully decentralized. One also needs to keep in mind that PoW has its own problems regarding energy extensiveness and scalability. Though Bitcoin's energy consumptiveness has been criticized in the past [2], the problem likely far extends energy consumption. The problem is likely that of computational efficiency. Competing forms of consensus that are sort of PoW-like, include PoST or "Proof of Space and Time" [3]. However, these likely formulate their own problems. PoST can still have an environmental impact or computational efficiency problem w/ specialized HDD or SSD storage devices, or they also have the problem of disenfranchising ASIC miners and other hardware. Therefore, the need for PoCP or Proof of Computation exists which is a form of verifiable computing storage [4] or hashing formulated in Lonero's HashBolt consensus. PoCP is seperate from Lonero's HashBolt and is just utilized in its experimental mining proof for its masternode consensus. PoCP is also a consensus being utilized in other cryptos including an under development experimental Bitcoin Fork (Bitcoin Efficient) and even BitBadges. Other technological usecases of Lonero are also being utilized including various sidechains in cryptocurrency or blockchain systems such as CloutContracts [5] . This is of importance given that both PoCP and being offline-first are core pieces of the blockchain design and architecture for BitBadges.

BitBadges is built off the idea of distributed identity and identity type ledgers. Think of identity as a permanently registered or issued NFT or hash establishing some sort of authoritative proof. These proofs are things such as "Proof of Identity" or "Proof of Ownership" stored permanently on the blockchain. Two crucial points of consideration are the storage method and the upgrades that have been happening on BitBadges over time. The first version of BitBadges or BitBadges 1.0 was built by Trevor Miller. BitBadges 1.0 provided a backbone for what BitBadges is and its core functionality. Hashes for issued badge identities or NFTs were stored permanently via IPFS, and posted on an account known as BitBadgesHash. BitBadges 1.0 had its core database hosted on Firebase, and integrated w/ BitClout. The core problem with the first variation of BitBadges was a decentralized idea and concept being built on and integrating centralized technology. This is why a major change has been proposed in regards to architecture and turning BitBadges into its own blockchain.

BitBadges 2.0 has been proposed and is being worked on by both me and Trevor as an updated architectural system centered around the core of what BitBadges is supposed to be. A core upgrade is that BitClout is to be looked at as more of a sidechain option amongst other cryptos, given that BitClout seems to be too technologically centralized. Also, firebase is being replaced w/ CouchDB to be more open-source, decentralized, and compatible w/ Lonero's decentralized-internet SDK. BitBadges is also being built to become its own blockchain and interoperable. It plans to have many integrations including a sidechain w/ CloutContracts (EthAuth Capabilities), and potentially integrate w/ TNB [6]. IPFS is also to be looked at as a sidechain integration option over the main hashing mechanism in relation to record or permanence. This is to be replaced w/ potentially Blake3 hashing via CouchDB which already stores the core data for BitBadges. Likely, 1 BitBadges coin would represent the ability to issue 5 badges as the core utility and monetization strategy. Creators can start building DeFi systems and even establish BitBadges as a form of value as well. A popular artist's single NFT may be worth 500 BitBadges hypothetically, or a university course issued as a badge may have had a 5 BitBadge issuing fee (just an example). Utility is core in regards to incentivising users and establishing well built ecosystems.

BitBadges 2.0 also plans on establishing some sort of proof validation or synchronized hosting system. This is where being PoCP and offline-first comes to play. Noteably, Blake3 is the chosen algorithm in regards to hashing. In regards to the database that stores the hashing, CouchDB allows for compatibility w/ the decentralized-internet SDK, which in terns allow for a process known as distributing sharding. The BitBadges blockchain can be synced peer 2 peer through a shared computing system creating a grid of shared computational power. Data can be synchornized in real time, and multiple nodes allow for further scalability and censorship-resistance. Proof validation is important in the fact that not only does BitBadges want to establish a shared economy of artists being rewarded, but it wants to expand its infastructure and reward those who help it expand. This process being done allows for this to happen in the most decentralized manner. In regards to PoCP, PoCP is being done in a way that is expandable across a wide range of hardware. BitBadges 2.0 also is becoming algorithmically optimized in regards to the hashing being tailored towards verified i.e centered around computational efficiency.

Privacy preservation is a key aspect in regards to how things are handled on the blockchain. For things such as identity and timestamps on ledgers, hashes are encrypted through the Blake3 algorithm and any private key is directly at the hands of the owner in regards to accounts. In regards to sidechain implementations, the same applies to the blockchain it is pegged w/, however, the hashing and data store method depends on which blockchain is being implemented. Users should always have their private key, and eventually algorithmic space-time complexity should increase dependent on the amount of nodes and activity within the network.

2.0 Design

There are multiple configurations to take into consideration in regards to the design for BitBadges 2.0. The design is centered around distributed computing and shared grid computing computational networks. Data syndicated through CouchDB and distributed through sharding is shared from one peer to another. Eventually, the main node shouldn't even need to be up in order for BitBadges to function as a network. Evidently, this is also an important feature in regards to scalability and prevention of having a single point of failure. As opposed to other decentralized and distributed systems, the core reliance is on the entire database and architecture as well as its hosting, this is opposed to a reliance on a small amount of nodes. BitBadges is built to be node-oriented and this is a core part of allowing the network to scale both through speed and architecture capabilities.

BitBadges wants to rely more on verifiable computing over staking or shared voting consensus mechanisms in order to perform two tasks optimally. One, is to prevent abuse. Two, is to be designed in a way that scales the architecture across multiple systems. Formulating a PoCP consensus allows for massive scalability and network verification without causing energy efficiency issues or slow speeds. The core is how can one build a decentralized system in a way that directly solves the missing link between centralized vs decentralized architecture so that eventually one can optimize speed and scalability.

2.1 Database

BitBadges 1.0 was based off of the following database schema [7], however this is really important in regards to the implications of what BitBadges 2.0 will host.

```
{
    attributes: string, //valid JSON object string; not currently implemented
    backgroundColor: string, //Valid HTML color name or hex string
    category: string, //not currently implemented
    collectionId: string, //not currently implemented
    dateCreated: Number, //number of milliseconds since UNIX epoch
    description: string,
    externalUrl: string, //must be in valid URL format
    id: string, // hash
    imageUrl: string, //please use permanent image storage solutions; badges are permanent
    isVisible: boolean, //currently always set to true
    issuer: string,
    issuerChain: string,
    recipients: string array,
    recipientsChains: string array,
    title: string,
    validDateEnd: Number, //number of milliseconds since UNIX epoch
    validDateStart: Number, //number of milliseconds since UNIX epoch
    validDates: boolean //true if badge has start/end dates, false if valid forever
}
```

Firstly, we want to focus on a few different variables. Attributes and everything related to ID is a given. However, what is unique to focus on in the schema, is the hash for that ID (which will likely implement Blake3) as well as the issuer, issuerChain, recipients, and recipientsChains. The issuer is the actual deployer address of said badge creator. The issuerChain can either likely be the direct mainnet of BitBadges or one of its networked pegs such as CloutContracts, BitClout, TheNewBoston (once available), etc. Then there are the recipient addresses and the tracking of badge issued hashes. All of these can be hosted for BitBadges 2.0 on a distributed CouchDB database w/ distributed sharding capabilities.

2.2 Model

A big aspect in regards to the model and design for BitBadges 2.0, is privacy be design [8]. Privacy by design meaning not in terms of just regulatory frameworks or how information is being processed, but the fact that everything is encrypted and data can be massively transmitted in a way that is transparent. Also hosting badge data isn't likely to be considered PII. Similar to other blockchain networks like Bitcoin, BitBadges 2.0 is very privacy-oriented. However, its node architecture allows it to be far more sustainable and be oriented towards node distribution. While luck chance validation is a large aspect in regards to traditional mining consensus, PoCP allows for more and more people to be franchised as part of the BitBadges 2.0 ecosystem. This is in part due to the daemon and its overall simplicity in its design.

2.3 Daemon

The daemon is the core piece of software that syncs the BitBadges 2.0 (BitBadges) node. This is what will allow for massive transmission of the data and distributed data sharding as well as shared/grid computing capabilities. The daemon performs the task of running the node syncing the CouchDB database and connecting within different peers of other daemons. The more and more daemons that run, the more and more the data is established through an offline-centric network. Eventually as more and more daemons are being integrated, BitBadges 2.0 can optimally be hosted without the core node being live. Privacy is still preserved and hashing is done through Blake3 in regards to issued badge and permanence. PoCP and the utilization of CouchDB to be able to integrate Lonero's decentralized-internet SDK, is what will allow for this to happen.

3.0 Architecture

PoCP allows for participation across multiple different devices and is similar to the distributed sharding mechanisms seen in programs like BOINC [9]. The behavior is that of a byzantine tolerant architecture [10] that is centered around shared computing. Other comparisons besides BOINC can perhaps be the SMesh Protocol [11], which was used in wireless mesh nodes. Most notably, when you allow for shared grid computing computational systems such as what is seen in BOINC, not only are you distributing data through data sharding mechanisms, but those who are building on top of your network can do the same. The same thing applies to the overall architecture and software that powers BitBadges 2.0. People can even create social networks on top of BitBadges and build various usecases for distributed ledger mechanisms and privacy-preserving sovereign identity.

4.0 Usecases

There are various usecases in regards to BitBadges 2.0 (BitBadges) that will be of technological value. For starters, the fact that 5 BitBadges may be worth the hypothetical right to issue a badge can establish a means of value for large scale DeFi-like applications in the future (as a technological utilizy). In regards to the architecture for BitBadges, it utilizes PoCP and the decentralized-internet SDK which creates an offline-centric network. Eventually badges can be issued in regards to forms of art, degree programs, certifications, health care databases and nodes, grid systems, etc. Currencies can even be established by means of worth in badges and one can create entire computational micro and macro-economies with BitBadges as a form of technological utility. Algorithms can even be built and distributed on top of BitBadges hash IDs and systems.

Conclusion

BitBadges 2.0 is a privacy-preserving blockchain system oriented around the use of badges. It is decentralized and establishes PoCP (Proof of Computation) while integrating CouchDB and the decentralized-internet SDK. BitBadges 2.0 is an improvement over BitBadges 1.0. BitBadges will integrate the Blake3 hashing algorithm for permanence and hash IDs. Five BitBadges will be hypothetically worth the right to issue a badge. This will allow for technological applications to also be built w/ BitBadges as a utility in the DeFi realm. The daemon will allow for massive node distribution, and BitBadges is trying to create an offline-centric network w/ byzantine tolerance-like performance in mind. It is a shared and grid computing network that implements distributing data sharding. A reward mechanism can be established for those who run nodes. Comparable architectures that aren't PoCP might include BOINC or the Smesh protocol. Numerous technological usecases such as distributed ledgers and digital certificates can be integrated on top of BitBadges being the utility.

Acknowledgements

I want to acknowledge Trevor Miller [12] who authored the original BitBadges and is the founder of BitBadges. He is collaborating with me on this project and also designed the original database schema being integrated for BitBadges. I would also like to acknowledge Lonero, BOINC, Smesh and other great projects within this community. I would also like to acknowledge the Chia network [13], that integrated and helped introduce Proof of Time and Space. Lastly, I would like to acknowledge Gridcoin [14] and Siacoin. These projects helped establish the foundation for what will likely be BitBadges 2.0's architectural design.

References

[1] Varshney, N. Why proof-of-work isn't suitable for small cryptocurrencies. TNW | Hardfork (2021). Available at: https://thenextweb.com/news/proof-work-51-percent-attacks. (Accessed: 10th September 2021)

[2] Aratani, L. Electricity needed to mine bitcoin is more than used by 'entire countries'. The Guardian (2021). Available at: https://www.theguardian.com/technology/2021/feb/27/bitcoin-mining-electricity-use-environmental-impact. (Accessed: 10th September 2021)

[3] Proof-of-spacetime: Coinmarketcap. Alexandria Glossary Available at: https://coinmarketcap.com/alexandria/glossary/proof-of-spacetime. (Accessed: 10th September 2021)

[4] Kamal, A. Proof of computation. PoCP Available at: https://lonero.org/pocp.html. (Accessed: 11th September 2021)

[5] CloutContracts. Home Available at: https://cloutcontracts.net/. (Accessed: 11th September 2021)

[6] Kamal, A. BitBadges TNB Integration (project proposal) · Issue #274 · Thenewboston-developers/projects. GitHub (2021). Available at: https://github.com/thenewboston-developers/Projects/issues/274. (Accessed: 12th September 2021)

[7] Miller, T. BitBadges Available at: https://bitbadges.github.io/. (Accessed: 12th September 2021)

[8] Privacy by design - the 7 foundational principles. Privacy by Design - The 7 Foundational Principles Available at: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/. (Accessed: 12th September 2021)

[9] BOINC projects. BOINC Available at: https://boinc.berkeley.edu/. (Accessed: 14th September 2021)

[10] Byzantine fault. Wikipedia (2021). Available at: https://en.wikipedia.org/wiki/Byzantine_fault. (Accessed: 14th September 2021)

[11] Smesh. SMesh Available at: http://www.smesh.org/. (Accessed: 14th September 2021)

[12] Trevormil - GitHub Available at: https://github.com/trevormil. (Accessed: 14th September 2021)

[13] Home. Chia Network Available at: https://www.chia.net/. (Accessed: 14th September 2021)

[14] Rewarding volunteer distributed computing. Gridcoin Available at: https://gridcoin.us/. (Accessed: 14th September 2021)

[15] Sia Available at: https://sia.tech/. (Accessed: 14th September 2021)