Radium Core: An Identity Management and Information Validity System

Justin Jacobeen
JustinJ100@gmail.com

Sajib Datta
sajib.datta@uta.edu

Preface. This paper assumes a previous understanding of blockchain technology, Proof-Of-Work, and Proof-Of-Stake. For more information on these topics, read the Bitcoin whitepaper, (Nakamoto, 2008) and the Black Coin Proof-of-Stake explanation (Earls, 2017).

1. Introduction

Blockchain technology provides a powerful new protocol for trustless data validation and verification. Bitcoin popularized this technology by creating a decentralized system to validate the history and authenticity of financial transactions. Much of the subsequent development around blockchain continued to focus on various implementation of financial systems, with little attention to other types of data validation. While projects that support non-currency uses of blockchain technology exist, substantial technical skill is required, rendering them inaccessible for many people. The Radium Project was founded to explore and develop non-financial types of data validation, and to make these functions available to the non-technical consumer. It is our goal to create an intuitive interface that provides users with access to a wide range of blockchain based functions. Currently, we are developing a suite of identity management, voting, and information validation tools.

2. Radium Blockchain

The Radium platform uses a Proof-Of-Stake blockchain based on Blackcoin, which was chosen as an energy efficient alternative to Proof of Work used by Bitcoin. Proof-Of-Stake saves a considerable amount of computational power and electricity compared to Proof of Work. While Bitcoin generates new blocks by the expenditure of computational resources (Nakamoto, 2008) Radium generates new coins by splitting groups of coins held in individual wallets (Earls, 2017). As the balance of a wallet increases, so does the probability of generating the next block in the chain and claiming the block reward. For the scope of this paper, a person attempting to generate new Radium blocks in order to claim the reward will be known as a "staker".

2.1 Spread Fees

All transactions on the block chain require the sender to pay a small transaction fee. This fee is intended to supplement the reward of the block in which the transaction is contained and to incentivize stakers to continue supporting the network. We theorize that because transaction fees may occur infrequently, each individual staker will have a low probability of generating a block with additional transaction fees. Unlike most blockchains where the transaction fees are included in the single block that contains the transaction, Radium spreads the fees over 1440 blocks. This helps to level the playing field and allow smaller wallets a better chance at receiving a share of the transaction fees.

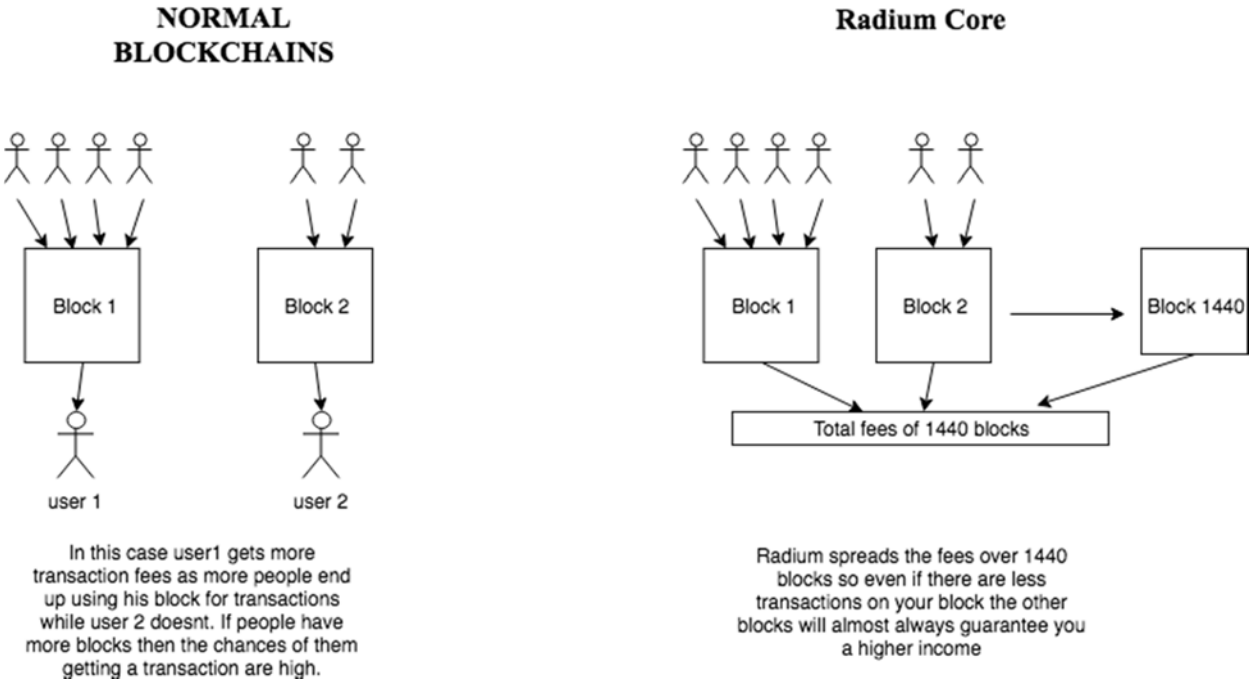

Figure 1: Spread Fees

3. Radium SmartChain

Radium SmartChain is the second component of the Radium system. It is a second layer of data within the Radium blockchain that contains all of the functions and validation information required for Radium's non-financial applications. Information is added to the SmartChain using specially formulated transactions with null data (op_return outputs) capable of storing information without impacting volatile memory usage (Apodaca 2017).

3.1 Identities

Today's online ecosystem is full of imposters, scammers, and hackers using fake websites, profiles, and identities for various nefarious purposes. Not only does this make it hard to avoid these malicious actors, it becomes challenging to locate authentic websites, retailers, and other online entities with whom a person would want to interact.

Radium Identities allow users to manage their own online presence in a way that creates a historical record of their activities secured in the blockchain in order to establish a pattern of trusted behavior. After creating an identity, a user can use that identity with all other Radium functions, including file signing and voting.

3.2 File Signatures and Tampering

Today's cyber-threat landscape poses a difficult problem for all organizations that need to safely and efficiently distribute digital files such as software and media. Security compromises resulting in unintentional distribution of malicious files can seriously damage an organization's reputation and can result in a lack of trust and loss of users.

Traditional methods of validating a file download are cumbersome and require that the user generate a checksum and manually compare the result with a checksum provided by the publisher. Using a combination of traditional file validation and blockchain signatures, Radium enables users to mark particular files as official or valid by signing them with a known Radium identity. Download providers, such as developers and digital media distributors can sign their offerings, allowing customers to prove that the files, programs, or media delivered are genuine and have not been altered by malicious actors in the delivery process. Consumers can then quickly validate files and receive an immutable, blockchain secured record about the origin of a file, who produced it, and at what time.

The difference is that Radium makes use of the immutability (Lewis, Antony 2016) of a blockchain, the guarantee that the data saved on a blockchain cannot be changed, to ensure that the checksum or keys that are stored have not been tampered with. A checksum value changes

every time the file is changed even a bit. Thus, most hackers make you download a malicious file, the checksum of the malicious file is different than the original. So, they also make sure that they change the original checksum value saved on the server with their new value. When people check if they downloaded the right file with the server, they get back a positive result. If you remove the possibility of the original value being changed, there is no other way left.

A common example of this is the Linux Mint website hack that is further discussed in our Use Case document (Use cases).

The reason why you need to check the checksum value is because you might be downloading a malicious file from some hacker. Most common way to make this happen is the Man In the Middle attack (Figure 2).

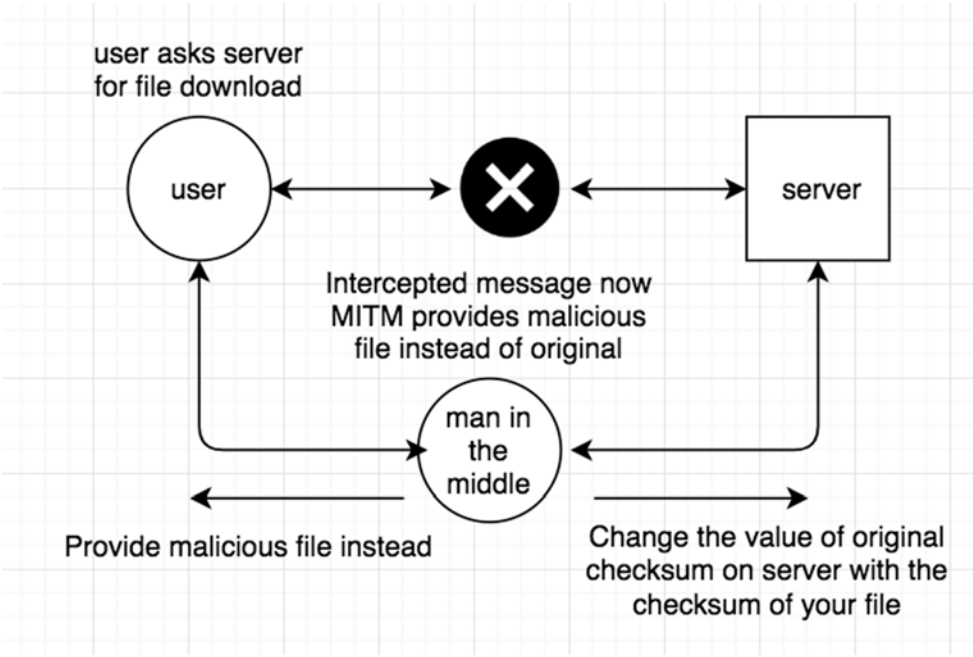

Figure 2: Man in the Middle Attack

This is countered by what people call certificates which are basically granted to the original website and if a hacker acts like the website you can immediately see he doesn't have a certificate of authority and recognize its fake. There have been incidents where hackers have acquired fake certificates from authorities either by tricking them (can be countered by the Radium Smart Chain Identity mechanism) or by infiltrating the authorities and acquiring one by themselves (can be countered by immutability).

3.3 Voting

From the time voting was first introduced in Greece by Cleisthenes in 508 BC, voting has served as the cornerstone of the democratic decision-making process. Unfortunately, many voting systems have been difficult to secure and scale, leading to recounts, contested results, and accusations of fraud. Radium Elections is a blockchain-based voting platform designed to restore confidence, transparency, and integrity to the voting process. All election data and votes are recorded on-chain, allowing for near-time observation, counting, and verification by any third party running the SmartChain application. Radium Elections are designed for applications ranging from project management and club votes, to political elections and shareholder voting. Simple, reliable and secure voting systems are a cornerstone of free governance, and the Radium Elections platform is available to anyone with a Radium Identity.

Real time voting results can be viewed while voting is in progress and final results are available immediately after the election closes. The election results, including individual votes, will remain secured in the Radium Blockchain and visible indefinitely.

3.4 Text Notes

Placing text into a blockchain is not a new idea. Having a platform that makes it simple and easy is Radium Notes. Users can insert small text notes directly into the Radium blockchain. Notes can be used to make predictions, endearments, or any other type of public statement that needs both security and immutability.

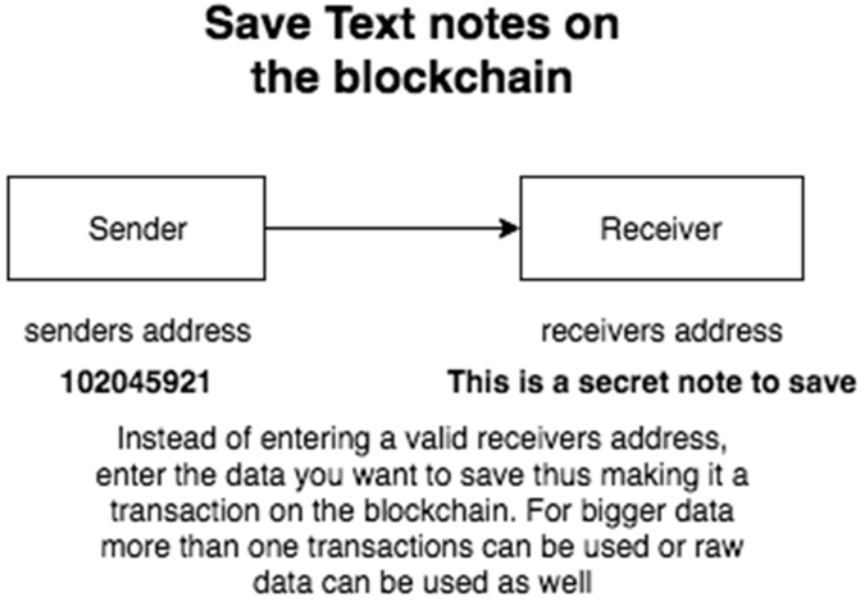

Figure 3: Saving Text on Blockchain

3.5 Custom Assets/Tokens

Custom Radium assets/tokens can be used for a wide range of purposes and act as their own cryptocurrency, while still running on the Radium blockchain. Unlike ordinary Radium (RADS), custom assets/tokens can be used to represent any kind of value.

4. Funding

From its beginning, the Radium Project has been funded solely by the developers and through donations of generous community members. The blockchain was launched with a fair Proof-Of-Work distribution phase before transitioning to Proof-Of-Stake. There was no premine, and no funds set aside for development. At the beginning the project was sustained by volunteer developers, as well as community members contributing to cover hosting and other infrastructure costs.

Unfortunately, this model has not proven to be sustainable, and the project found itself in need of funding. The idea of a development fund, funded by a percentage of the block reward, was brought to the community and approved using the existing blockchain voting system.

4.1 Development Fund

The Radium Development fund will be a 5 of 12 multi-signature address, with keys held by the core developers as well as several long-standing community members. Approximately every 7 days, a lump sum of tokens equal to 12% of the total network generation for that period will be created and sent directly to the development fund. The funds will be used primarily for, but not limited to hiring additional developers, legal counsel, and paying for infrastructure such as hosting and virtual servers.

All major disbursements will be put to a vote, allowing community members the opportunity to approve or disapprove the proposed use of funds. Disbursements from the fund will require five signatures from the key holders in order for the funds to be sent from the multi-signature address.

If excessive tokens reside in the development fund, they can either be destroyed or returned to the stakers using the Spread Fee protocol. In the event the coins are to be burned, they will be sent as a null data output, rendering them unspendable. If the tokens are to be returned to the stakers, they will be spent in a series of high-fee transactions, causing the block rewards to increase for a period of 24 or more hours.

More info on the exact key holders or statistics can be found at the development fund section on the website. (Funding).

5. Zero Client

The Zero Client (ZC) User Experience (UX) is a work in progress and designed to facilitate accessibility to the SmartChain utility using a purely web-based interface. The web interface does not require any installation, or downtime for syncing which could be in hours. All Radium SmartChain functionality is available for use within the ZC and eliminates the need for an end-user to acquire Radium (RADS) in order to utilize the SmartChain.

6. Conclusion

This paper has described an identity management and information validity system built upon a Proof-Of-Stake blockchain. We discussed the goal of making these and other non-financial blockchain secured functions available to the general public. Included was an explanation of how Identities, File signatures, Voting, and Text notes interact to form the complete Radium system. The financial status including the fair Proof-Of-Work launch and need for additional funding was discussed along with the proposal of supporting future development by placing 12% of total tokens generated into a development fund.

References

1. S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

2. J. Earls, “The missing explanation of Proof of Stake, Version 3,” http://earlz.net/view/2017/07/27/1904/the-missing-explanation-of-proof-of-stake-version July 2017.

3. R. Apodaca, “OP_RETURN and the Future of Bitcoin,” https://bitzuma.com/posts/op-return-and-the-future-of-bitcoin/ , September 2017.

4. Lewis, Antony. “A gentle introduction to immutability of blockchains,” https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/, February 2016.

5. RadiumCore. “Radium UseCases,” https://radiumcore.org/radium-smartchain-use-cases/

6. RadiumCore. “Radium Development Fund,” https://radiumcore.org/development-fund/