Validity: A Digital Value Transfer and Information Verification System

The Validity Contributors

Preface. This paper assumes a previous understanding of blockchain technology, Proof-of-Work (PoW), and Proof-of-Stake (PoS). For more information on these topics, read the Bitcoin whitepaper [1] and Proof-of-Stake explanation [2].

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. The Validity project was founded to develop both financial and non-financial types of data validation, and to make these functions available to the non-technical consumer. The goal is an intuitive interface that provides and empowers users with access to a wide range of blockchain based functions including (but not limited to) identity management, voting, and information validation tools.

2. Validity Blockchain

2.1 Launch

The Validity blockchain officially and publicly launched on the 25th of May 2015 and has been working as intended ever since. There was an initial Proof-of-Work phase that lasted for 10 days after which the network switched to Proof-of-Stake. There was no initial coin offering (ICO), no pre-sale and no pre-mine. It was an 100% fair launch announced to the public in advance.

2.2 Rebrand

Originally, the technology was dubbed xRadon and a rebrand to Radium happened on the 18th of January 2016.

2.3 Tokenomics

The word "tokenomics" is a combination of the words "token" and "economics" and it is a relatively new term that rose to popularity in the middle of 2017. Tokenomics encompasses the concept of the study, design, and implementation of an economic system to incentivize specific behaviors in a community, using tokens to create a self-sustaining mini economy. It includes game theory and mechanism design.

2.3.1 PoSv3

The Validity platform uses a Proof-of-Stake (PoSv3) 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 [1], Validity generates new tokens (VAL) by splitting groups of tokens held in individual wallets [2]. 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 Validity blocks in order to claim the reward will be known as a "staker".

In conclusion, a Proof-of-Stake system is more environmentally friendly and efficient, as the electricity and hardware costs are much lower than the costs associated with mining in a Proof of Work system. The low barrier to entry encourages a greater number of people to run nodes and get involved because it is easy and affordable to participate in the Validity Proof of Stake system; this results in more decentralization.

Figure 1: Proof-of-Stake Consensus

2.3.2 Monetary Principle and Limited Supply

The VAL token is a better form of money, based on savings rather than on debt. It is influenced by John Nash's fundamental contributions to game theory and his paper on 'Ideal Money' [3].

Gresham's Law is a monetary principle stating that "bad money drives out good money". Validity doesn't aim to be an electronic cash system (bad money), rather it aims to be a scarce digital asset (good money) that provides advanced utility. The maximum supply is capped at 9 million tokens.

Thiers' Law argues that bad money would drive good money to a premium, rather than driving it out of circulation. However, Thiers' Law ignores the influence of legal tender legislation, which requires people to accept both good and bad money as if they were of equal value. People tend to keep the money of greater perceived value in their possession and pass on the bad money to someone else.

2.3.3 Validity PoS Reward Structure

Instead of Bitcoin's model which cuts the supply of newly mined tokens in half every four years, Validity provides a more stable decrease of newly generated supply over time. Once the maximum supply of 9 million tokens is reached, it is assumed that the transaction fees will be rewarding enough to incentivize stakers to keep on validating transactions. The following emission schedule was implemented in August 2018 (start of year 1):

Year	Stake Reward Per Block	Dev Fund Allocation Per Week	Dev Fund Allocation Per Block	Total Generation Per Block	Reward Period (Days)	Coins Per Period
1	0.5	600	0.062111801	0.562111801	365	283135.7143
2	0.48	582	0.060248447	0.545248447	365	274641.6429
3	0.47	565	0.058488613	0.528488613	365	266199.7143
4	0.456	548	0.056728778	0.512728778	365	258261.4857
5	0.442	532	0.055072464	0.497072464	365	250375.4
6	0.429	516	0.053416149	0.482416149	365	242993.0143
7	0.416	501	0.051863354	0.467863354	365	235662.7714
8	0.404	486	0.050310559	0.454310559	365	228836.2286
9	0.392	471	0.048757764	0.440757764	365	222009.6857
10	0.38	457	0.047308489	0.427308489	365	215235.2857
11	0.369	443	0.045859213	0.414859213	365	208964.5857
12	0.358	430	0.044513458	0.402513458	365	202746.0286
13	0.347	417	0.043167702	0.390167702	365	196527.4714
14	0.337	404	0.041821946	0.378821946	365	190812.6143
15	0.327	392	0.04057971	0.36757971	365	185149.9
16	0.317	380	0.039337474	0.356337474	365	179487.1857
17	0.307	369	0.038198758	0.345198758	365	173876.6143
18	0.298	358	0.037060041	0.335060041	365	168769.7429
19	0.289	347	0.035921325	0.324921225	365	163662.8714
20	0.28	337	0.034886128	0.314886128	365	158608.1429
21	0.272	327	0.033850932	0.305850932	365	154057.1143
22	0.264	317	0.032815735	0.296815735	365	149506.0857
23	0.256	307	0.031780538	0.287780538	365	144955.0571
24	0.248	298	0.030848861	0.278848861	365	140456.1714
25	0.241	289	0.029917184	0.270917184	365	136460.9857
26	0.234	280	0.028985507	0.262985507	365	132465.8
27	0.227	272	0.02815735	0.25515735	365	128522.7571
28	0.22	264	0.027329193	0.247329193	365	124579.7143

Figure 2: Validity PoS Reward Structure

2.3.4 Spread Fees Protocol

All transactions on the blockchain 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. 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, Validity spreads the fees over 1440 blocks. This helps to level the playing field and allow smaller stakers a better chance at receiving a share of the transaction fees.

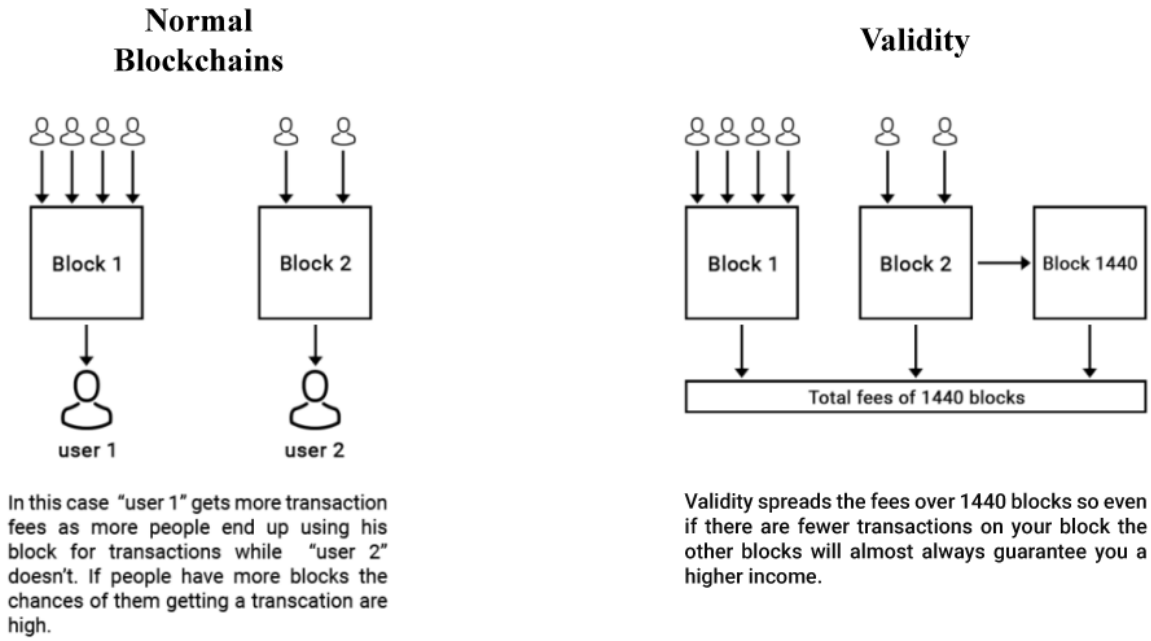

Figure 3: Spread Fees Protocol

2.4 Atomic Swap Compatible

An atomic swap is a smart contract technology that enables the exchange of one cryptocurrency for another without using centralized intermediaries, such as exchanges.

Not all cryptocurrency exchanges support all tokens. As such, a trader wishing to exchange one cryptocurrency for another one that is not supported on the current exchange may need to migrate accounts or make several conversions between intermediate tokens to accomplish this goal. There is also an associated counterparty risk if the trader wishes to exchange his or her tokens with another trader.

Atomic swaps solve this problem through the use of Hash Timelock Contracts (HTLC). As its name denotes, HTLC is a time-bound smart contract between parties that involves the generation of a cryptographic hash function, which can be verified between them.

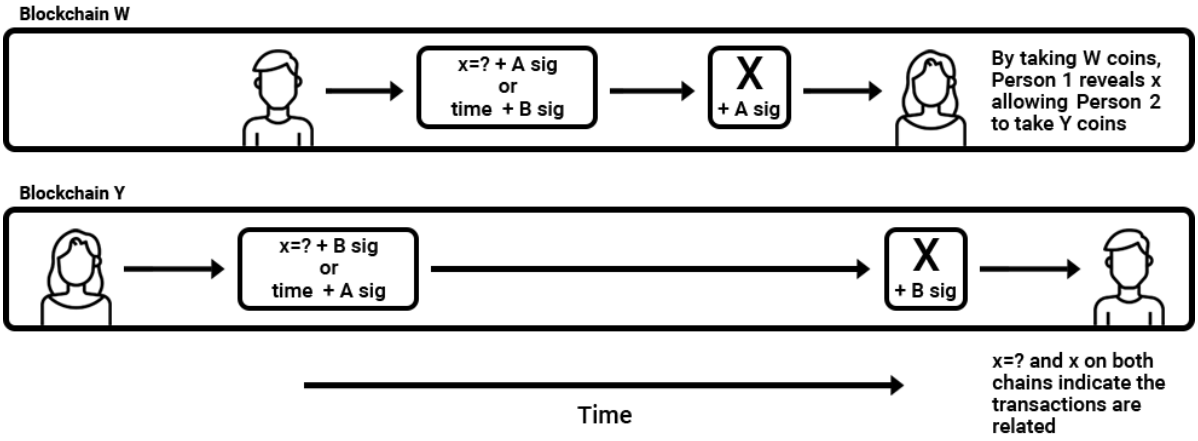

Figure 4: Atomic Swaps

2.5 Scaling Validity

Blockchains suffer from what is known as ''The Scalability Trilemma''. A blockchain can only at most have two of three properties: scalable, secure and decentralized. Satisfying all three at the same time is difficult, although we are getting close. The Validity blockchain combines scaling the protocol level (SegWit) and Layer 2 solutions (Smartchain).

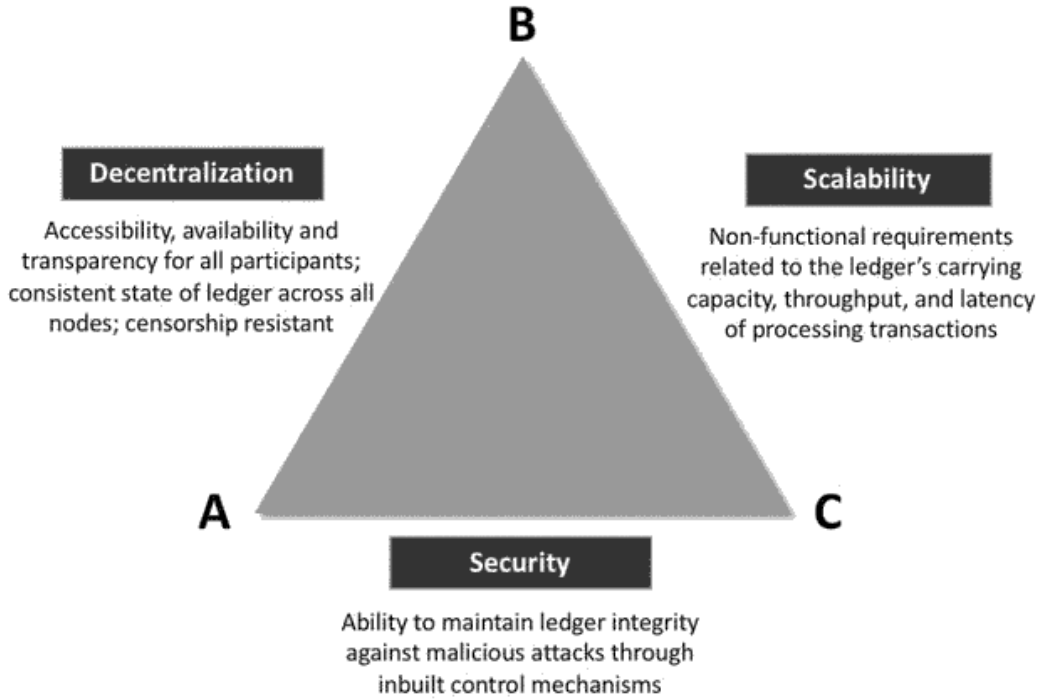

Figure 5: The Scalability Trilemma

2.5.1 Segregated Witness (SegWit)

SegWit is the process by which the block size limit on a blockchain is increased by removing signature data from transactions. When certain parts of a transaction are removed, this frees up space or capacity to add more transactions to the chain.

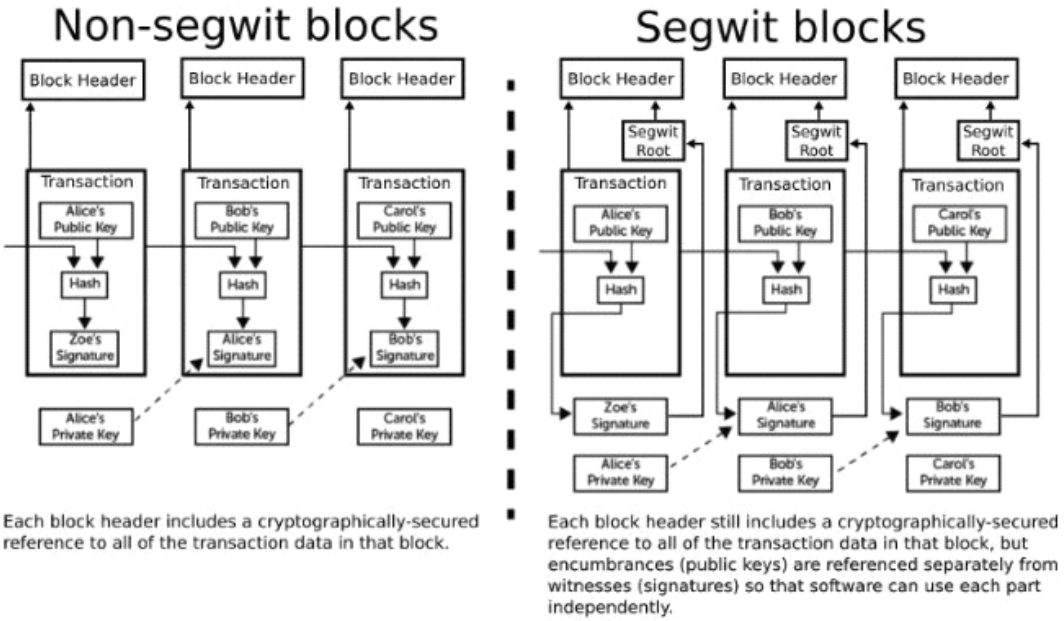

Figure 6: Segregated Witness (illustration posted by David A. Harding)

2.5.2 Layer 2 Solutions

Layer 2 refers to a secondary framework or protocol that is built on top of an existing blockchain system. Layer 2 solutions don't increase the throughput, rather they move some of the transactions (data) off the chain. For this reason, these techniques may also be referred to as "off-chain" scaling solutions.

One of the main advantages of using off-chain solutions is that the main chain doesn't need to go through any structural change because the second layer is added as an extra layer. As such, layer 2 solutions have the potential to achieve high throughput without sacrificing network security.

In other words, a great portion of the work that would be performed by the main chain can be moved to the second layer. So while the main chain (layer 1) provides security, the second layer offers high throughput, being able to perform hundreds, or even thousands, of transactions per second.

2.6 Open Source

The Validity blockchain is open source software and is collaboratively produced, shared freely, published transparently, and developed to be a community good rather than the property or business of a single company or person.

3. Validity SmartChain

The Validity SmartChain is the second component of the Validity system. It is a layer 2 solution of data within the Validity technology suite that contains all of the functions and validation information required for Validity'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 [4].

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. Validity 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 Validity functions, including file signing and voting.

3.2 File Signatures

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, Validity enables users to mark particular files as official or valid by signing them with a known Validity 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 with Validity is that it makes use of the immutability [5] of the blockchain 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 little. Thus, most hackers make you download a malicious file, the checksum of which is different from the original. To camouflage this, they also make sure that they change the original checksum value saved on the server to match their new value. When the user checks whether they downloaded the right file with the server, they get back a (false) positive result. If the possibility of the original value being changed is removed, the hacker's strategy cannot work.

The most common technique used by hackers is the **Man In the Middle Attack**: see **Figure 7** below.

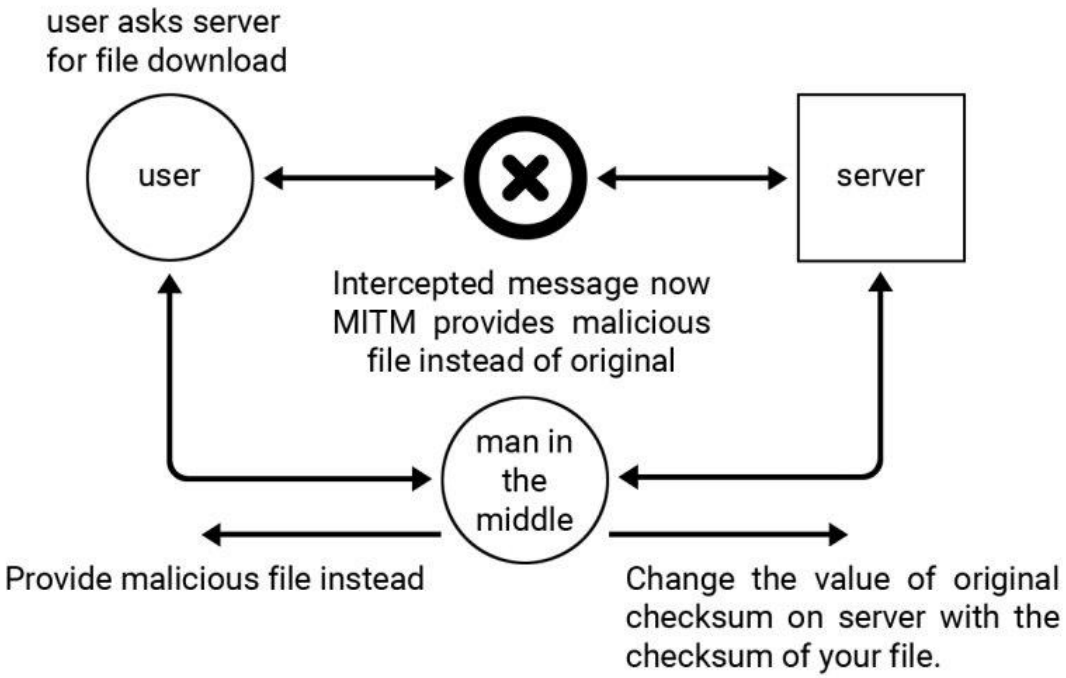

Figure 7: Man in the Middle Attack

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/she 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 Validity SmartChain 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. Validity 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. Validity 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 Validity Elections platform is available to anyone with a Validity 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 Validity 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 Validity Notes. Users can insert small text notes directly into the Validity blockchain. Notes can be used to make predictions, endearments, or any other type of public statement that needs both security and immutability.

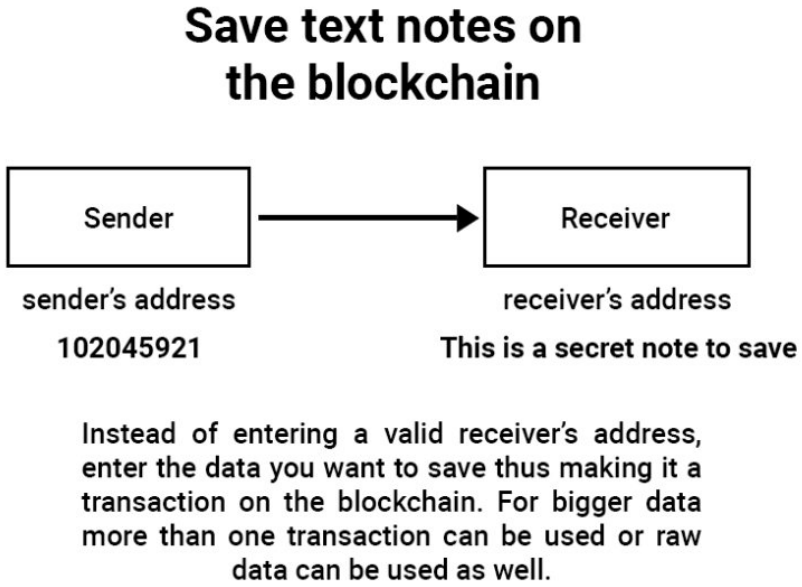

Figure 8: Saving text notes on the Validity blockchain

3.5 Custom Assets/Tokens

The tokenization of assets refers to the process of issuing a blockchain token (specifically, a security token) that digitally represents a real tradable asset. Such a security token (STO) created on the Validity Smartchain could represent a share in a company, ownership of a piece of real estate, or participation in an investment fund. By tokenizing assets—especially private securities or typically illiquid assets such as fine art—these tokens can then be traded on a secondary market of the issuer's choice.

An STO is capable of having the token-holder's rights and legal responsibilities embedded directly onto the token, along with an immutable record of ownership. These characteristics can add transparency to transactions, allowing you to know with whom you are dealing, what your and their rights are, and who has previously owned this token.

3.6 Trusted Diplomas and Certificates

In the last 10-15 years we have witnessed an increase in falsified academic credentials. This trend poses a serious, prevelant and ever-increasing problem on a global scale. For universities, fake qualifications pose a reputational risk – within other academic institutions and in the workplace. For employers, hiring those who have falsified their qualifications or lied on their CVs can lead to costly exposure to legal action, high staff turnover, lost revenue and public reputational damage which may take years to repair.

The Validity Smartchain offers universities and educational establishments to have an immutable record on the Validity blockchain that cannot be tampered with. Employers can easily verify a candidate's record, making it an efficient tool to combat fraud. Data records can be encrypted and stored on the Validity blockchain while file records would be encrypted and stored locally or on the Inter-Planetary File System (IPFS) with their respective hashes.

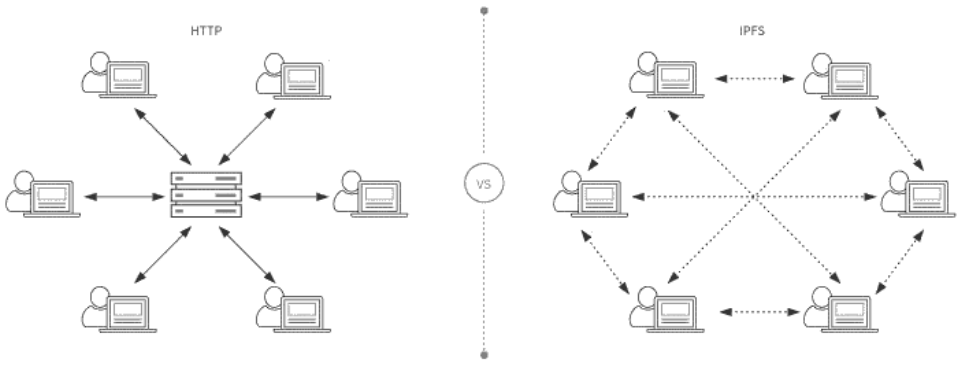

Figure 9: HTTP vs IPFS

A VAL allotment is recommended to begin operations. This would allow educational establishments to operate

in a self-sustainable fashion wherein the VAL allotment could be staked via the Validity Proof-of-Stake consensus algorithm resulting in additional VAL to fuel operations whilst also helping to secure the entire network. Moreover, as operational costs on the SmartChain are minimal, the initial allotment should last for years, if not indefinitely, when combined with staking.

3.7 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 Validity SmartChain functionality is available for use within the ZC and eliminates the need for an end-user to acquire Validity (VAL) in order to utilize the SmartChain.

4. Funding

From its beginning in 2015, the Validity project has been funded solely through donations and 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.

4.1 Development Fund

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

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 tokens 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.

4.2 Donation Fund

In addition to the Development Subsidy introduced in the August 2018 hard fork, we have also established a general donation fund for the Validity project's ongoing and ever-expanding needs. While the development subsidy does help, donations into this fund are always welcome and very much appreciated:

Bitcoin donation address: 18JNKxDgX1ebuwmT3qKjrvKxeSwxBXjR41

Validity donation address: QVZ419DruuEQYxbCgvF6vNwYTJizbhC9qw

Conclusion

This paper has described a digital value transfer 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, Custom Assets, Trusted Diplomas & Certificates and immutable Text Notes interact to form the complete Validity system. The history of the project, the financial status including the fair Proof-of-Work launch, and the need for funding which resulted in the creation of the development fund was discussed.

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] John F. Nash, "Ideal Money and Asymptotically Ideal Money, Contributions to Game Theory and Management," 2009.

[4] Richard L. Apodaca, "OP-RETURN and the Future of Bitcoin," https://bitzuma.com/posts/op-return-and-the-future-of-bitcoin/ September 2017

[5] Antony Lewis, "A Gentle Introduction to Immutability of Blockchains," https://www.linkedin.com/pulse/gentle-introduction-immutability-blockchains-antony-lewis March 2016.