ABSTRACT

The writer’s launch Wiz, a service that allows users to store their data in a distributed manner Storage (Wiz) contracts may be established between peers using Wiz opens up the possibility for other services to come together and coordinate their storage capacities. Storage arrangements specify the type of data to be processed and the associated cost. For the customer to be sure that their data is being retained, they must show proof of storage to the data storage provider at specific intervals. Contracts are kept in a shared ledger so that they can be openly scrutinized and corrected by all. Wiz may be considered a cryptocurrency that supports all kinds of contracts. Wiz would first be offered as an alternative to Bitcoin but later merged with the Bitcoin community.

INTRODUCTION

Wiz has set out to deal with current cloud computing at both the consumer and business stage. Instead of purchasing from traditional storage providers, peers to themselves instead, Wiz relies on individuals to store their peers. Wiz can only keep contracts, setting out the terms and conditions under which the service provider and client can engage in business. This is analogous to how Bitcoin's network is used. The database service provider (also known as a host) promises to retain the data for the term of the deal and periodically offer evidence of continued storage. Authors are paid for any manuscript they send and penalize for failing to meet the required number of proofs. Since these proofs are accessible in the database, WizCoin can use an automated agreement system to execute storage contracts. Importantly, this ensures that clients do not need to perform storage proofs. No matter where we store records, it provides a low assurance of capacity, bandwidth, or service efficiency. Instead, we advise the use of keeping redundant data on different host locations. The employment of error-correction codes yields exceptional reliability without unnecessary redundancy. Wiz would be initially introduced as an altcoin with a decentralized cryptocurrency platform. Using a two-way peg for the Bitcoin blockchain is under consideration, as detailed in "Enabling Blockchain Innovations in the Enterprise with pegged sidechains." This is much the same as the procedure followed by Bitcoin except for the differences mentioned below.

GENERAL STRUCTURE

The only difference between Wizcoin and Bitcoin is in the transfers. Diverse transaction options such as pay-to-to-public-key and pay-to-script-hash are allowed by bitcoin's scripting framework. Instead of using the scripting technique, Wiz utilizes an M-of-of-N signature scheme on all transactions. It makes it simpler and safer. Additionally, smart contracts have contract functions to execute trades and create and implement storage contracts. A project can be extended in three ways: a lease, proofs, contract revisions, and contract changes. On the form in question, you state your understanding of the amount of storage you will use and the file's content in advance. They measure the reliability of a host regarding how well a host would comply with proof-of-storage requirements. After documents are drafted, they may be amended with contract modifications. Section 4 defines the primary forms of transactions. Section 5 contains general information.

TRANSACTIONS

A transaction contains the following fields:

Field	Description
Version	The version number of the system's software (think of it as a two-digit integer representation of a name/adjective describing your personality).
Arbitrary Data	Used for metadata or otherwise
Miner Fee	The reward is given to a miner
Inputs	Incoming funds
Outputs	Outgoing funds (optional)
File Contract	See: File Contracts (optional)
Storage Proof	See: Proof of Storage (optional)
Signatures	Signatures from each input

INPUTS AND OUTPUTS

Outputs have several coins. For each production, there is a transaction that it is linked to. Transaction t's output id is H("t" output" " " "output" " I denotes " These two variables are distinct since W(W(w) transaction), and M(m) have a transaction. The output IDs for H(W(w) and m transactions are given by An entry. Roughly speaking, there are two kinds of input and output scenarios. As one of the inputs has to spend requirements as part of its definition, the Merkle root should be part of the definition of output.

SPEND CONDITIONS

Prerequisites are necessary criteria that can be expended only if they are fulfilled. In this case, the money you would pay is often locked in and defined as well as the number of signatures. The last performance cannot be expended before at least as many keys have signed. As part of the spend requirements, the total funds, along with the timestamp lock, are hashed into a Merkle tree using the public keys, the number of signatures needed is specified. The root hash is the address that this transaction is linked to. To spend the bitcoins, you must have the relevant address details. A Merkle tree helps you to use conditions to disclose details selectively. WizCoin may release a time lock without showing how many public keys are required. WizCoin should remember that the period and quantity of signatures must be considered while trying to brute-force these hashcodes. WizCoin may add more entropy without growing the size of these fields.

SIGNATURES

Each transaction input must be signed before it can be processed. It is chained with an input ID, a timestamp, and a signed bits of the transaction, which parts have been validated and which are deemed valid. The signature applies to which device. It is based on the date and time that the signature becomes valid. Except for the signature, any of the transaction fields can be signed (as this would be impossible). If the transaction should be signed except for the signatures, there is a "Flag All Except for Signatures" checkbox. For transactions that go deeper, this supports a wider variety of scenarios. All authenticated fields must be included in the actual data signature; the signature, then, consists of the time lock, the input ID, and all the flags. every signature on the document is required

FILE CONTRACTS

The root of the file is the Merkle tree hash. This hash is constructed by segmenting the file into constant-sized chunks and producing a Merkle-tree. It is possible to compute the root hash and the total file size when using this method. Another common term the reviewer will use is bonuses. File contracts define a reward for a correct answer, the reward for an incorrect or missing answer, as well as the maximum number of mistakes that may be allowed. The challenge frequency dictates how frequently a host must provide storage proofs and creates discrete proof windows (one warranty per window). If you have successfully found valid evidence, payment will be made to you during the challenge window. "Raconteurs are storytellers; we know the raconteur long enough to forgive them for what they don't know (presumably the host). That person. If the best evidence has not been submitted at the end of the challenge period, a prize is provided to the unsuccessful participant, "is located in the centre of the brain. The centre of the brain has an expanded cerebral cortex, which is necessary for its well-being. A set limit on the number of proofs established in terms of the contract is specified in these rules; if this is reached, the warranty is void. If the agreement is still running at its term's expiration, then all coins go to the actual recipient. Alternatively, if the contract has used up all of its funding or if the number of missed proofs is reached, the contract will end in a failure, and the funds are refunded to the investor. by placing an X or not placing an X in the contract makes a new transaction output belonging to the specified recipient. For proof, the output ID is based on the contract ID, which is defined as

$H(\text{transaction}jj\backslash\text{contract}"jji)$

Where i is the index of the contract within the transaction. The output ID of the proof can then be determined from:

$H(\text{contract ID}jj\text{outcome}jjWi)$

W*i* is the window index, i.e. the number of windows that have elapsed since the contract was formed. The outcome is a string literal: either \validproof" and \missedproof", corresponding to the proof's validity.

The output ID of the contract termination is defined as:

H(contract ID*jj*outcome)

Derived from "We extract the expressions "succeeding" and "failing" from the words "performance" and "failure." A library often includes a collection of editing requirements, which are generated by a set of listings, which could involve a range of items with features "the same as in the case of a transaction's pending status WizCoin must fulfil the terms to amend the deal. The contract funds, the file, and output addresses are all available for modification. After you make these modifications, WizCoin must rechallenge all storage proofs before WizCoin can accept them. Theoretically, micro-edits could be caused by peers "[Besides,] WizCoins enhanced the size of the team to help improve the frequency of frequent editing.

PROOF OF STAGE

The idea is to periodically file proof transactions to satisfy file contracts. Each contract requires storage proof. A storage proof does not require an agreement ID and proof data.

ALGORITHM

The final verification stage consists of providing a link to the original file and a list of Merkle trees, demonstrating that all links are intact. This section is original. Statements about bitcoin are recorded on the bitcoin database, so you will see whether they are true or not. Only a segment of data is used in each storage proof, which is also randomly selected. The random challenge ID is computed as H(Contract ID JJ(Window - 1)) using the window number j as the previous block.

In short, if the host consistently displays random sections, then it is very likely that they have the whole file. When only half of the data on a file is available, it is impossible to perform about half of the verification steps.

BLOCK WITHHOLDING ATTACKS

The random number generator is subject to manipulation via block withholding attacks, in which the attacker withholds blocks until they find one that will produce a favourable random number. However, the attacker has only one chance to manipulate the lucky number for a particular challenge. Furthermore, withholding a block to use the random number will cost the attacker the block reward. If an attacker can mine 50% of the blocks, 50% of the challenges can be manipulated. Nevertheless, the remaining 50% are still random, so the attacker will still fail some storage proofs. Specifically, they will fail half as many as they would without the withholding attack. To protect against such attacks, clients can specify a high challenge frequency and hefty penalties for missing proofs. These precautions should be sufficient to deter any financially-motivated attacker that controls less than 50% of the network's hashing power. Regardless, clients are advised to plan around potential Byzantine attacks, which may not be financially motivated.

CLOSED WINDOW ATTACK

It is only possible for hosts to sign the storage proof if their transaction is confirmed in the blockchain. You could eliminate storage fees for miners by removing guarantees from the blocks but would incur a penalty on other hosts. Alternatively, a hefty price to store proof of deposit could serve as a form of miner blackmail. The well-known malefactor is known as a closed window attack." Also, this argument would employ large windows. They have a reasonable expectation that a certain percentage of participants will use their proofs in transactions for compensation. It is assumed that a host freely agrees to all file contracts, allowing them to cancel any contract that leaves them open to security breaches.

ARBITRARY TRANSACTION DATA

Each transaction has a fixed piece of information that can be used for any purpose. There must be a signature in the trade for arbitrary data to be stored. In the beginning, nodes can be able to accept 64 KB of random data per block. By creating this opaque data, the hosts and clients are now allowed to self-organize more creatively. Once you have it running, you can use it for advertising available space or files in need of a host or set up a decentralized tracking service. Users can select arbitrary data for this implementation of soft forks. This would be an "anyone can play, but only if they meet the restrictions stated in the arbitrary data" without being able to transfer the file. Miners who understand the stipulations can delay or cancel any outgoing transaction. Serotonergic nodes will keep in step with unparseable data.

STORAGE ECOSYSTEM

Wiz project relies on a distributed storage ecosystem that's fostered cooperation rather than competition. An arbitrary data field may be employed by storage providers in the networking strategy to announce their presence. This can be used with clear, client-oriented templates to do. Clients can make these announcements and only those that they trust.

HOST PROTECTIONS

A contract must allow the storage provider to reject unfavourable terms or illegal files because of host protections. All of the data must be available when the provider agrees to the contract. Storage terms allow a measure of flexibility. They can be hired to publicize themselves, offer a low penalty and lower loss of data, or be employed to promote themselves, offering harsher penalties. A market that maximizes the use of storage strategies will be the most efficient. The attacker has found a way to trick the hosts into thinking that their storage proofs or files are unavailable. An intruder can launch an attack on either a client or a server; it is the host's responsibility to take the appropriate measures to keep the other safe.

CLIENT PROTECTIONS

Even if the host disappears, the data remains secure thanks to erasure codes like regenerating codes. Principles of this type usually work by breaking the file into m pieces, and each piece may have a unique code. Based on the erase code and redundancy factor, the values for n and m vary. After that, each piece is encrypted and then saved to many locations. Increasing the average file availability improves the overall capacity. As an extreme example, if it only needs 10 out of the most reliable hosts to succeed, the client has demonstrated a very high degree of trust in them. Rehoming can help even further by finding new locations for file pieces whose current location has failed. Metrics can also benefit from this strategy; the client may reduce latency by obtaining the most recent content from 10 proximity servers. This may increase the speed of receiving content by using the fastest. It can be done to improve bandwidth utilization by running these at the same time.

UPTIME INCENTIVES

Your storage will have no method of reliably staying up, which means you will have no way to enforce the industry standard of having a 99.999% uptime. No such provisions demand is required of hosts to allow users to be met. Thus, clients would assume that web hosts are holding their files for ransom and demanding high fees to get them back. It can be, however, because of erasure codes. Customers have the freedom to work only with cooperative hosts, rather than wasting time on uncooperative ones. Subsequently, the client gets more power, and the upload charge goes away. When we examine this scenario, we see that clients have an incentive to send you a file, and hosts need to supply the best service. A website client may make a file request anytime, driving the Web Hosts to maximize uptime to maximize rewards. Clients can motivate higher transaction volumes and lower processing time by more enormous reward incentives. Also, customers may engage in "microscale" surveys, even if they aren't downloading anything. However, it is essential to keep in mind that these uptime incentives are strictly part of the Wiz framework. You must pay before downloading, such as by micropayment. Micropayments allow clients to make any payments without requiring high transaction volumes, increasing the blockchain's lag and transaction load. You could select a small part of the file to have transferred and then wait for a micro-payment to be received. The many payments allow each party to cut their losses to a

minimum. It can make payments every few seconds without affecting throughput due to micropayments.

BASIC REPUTATION SYSTEM

Only the best hosts will do. An examination of their past does not yield accurate results because it could be falsified. Contracts with itself about huge "fake" files such as zero files one could carry out storage proofs on non-trivial data if one only didn't need to store anything. It is recommended that clients issue large volumes of time-locked coins and require them to identify themselves in the ECDSA-propagating part of the BGP route announcements to stave off this Sybil attack. By doing this, the above calculation, the host has locked 140 days' Mitigating Sybil-style attacks is easier for high-value clients because valuable locks are harder to come by. Clients can design their formula for finding hosts and include factors such as price, storage volume, and the likelihood of losing files when picking them. This could use human review or other metrics to improve a more centralized system.

Wiz FUNDS

Wiz is an alias of Neato Robotics, which the ever-creative Software Development Corporation owns. Nebulous has always intended to be for-profit, and Wiz aims to make money for the company. It's not a dependable source of income because it requires the company to introduce a new currency, and the increasing value of that currency ties its revenues to the company. The organization needs to use money that comes in one way or another as income must go out another way or route. Also, suppose a large amount of the currency is controlled by a single entity. In that case, it gives the owner or founders an enormous advantage over others and a degree of power, and they could be highly disruptive in the market. In short, Wiz wants to raise revenue in a manner proportional to the value Wiz adds to its customers' contract. This is achieved by charging administrative fees on all warranties. By the terms of the agreement, 3.9 per cent of the funds are distributed to WizCrowds shareholders. Initial public investors will hold approx. 88% of the shares in the company, while Nebulous Inc. will initially control the remaining stock. Wizfunds can be sent to other addresses in the same way that Wizcoins can be sent to different addresses. To use them in contracts or to pay miner fees is not permitted, though. When Wizfunds are transferred to

a new address, an additional unspent output is created, containing all of the Wizcoins earned by the Wizfunds since their previous transfer. These Wizcoins are sent to the same address as the Wizfunds.

ECONOMICS OF WIZ

One of the critical measures of influence in the company is the value your work has for Wiz in producing new Wizcoins. This is likely to result in a permanent rise in the number of Wizcoins, and any additional coins would be distributed to miners as a pro-distribution. The first 300,000 coins will be produced. The amount will decrease by one coin per block until it reaches a minimum of 30,000 and then remains there until inflation occurs. Following 10 minutes of rest, the annual increase in production is approximately 10%:

Year	1	2	3	4	5	8	20
Growth	90%	39%	21%	11.5%	4.4%	3.2%	2.3%

One of the drawbacks of the reward strategy is its inefficiency. Wiz aims to provide a public ledger with data management agreements. , the mining payout is linked to the overall market value of contracts only through a two-way linkage, not a one-to-one. For the short term, the Wizcoin is expected to be highly volatile. If the currency moves during the deal, the hosts could lose capital. Because of this, we hope to see the price of long-term contracts rising in the long term to reflect the risks associated with long-term contracts. Besides, hosts can list their rates in a more flexible currency (such as USD) and enter into contract negotiations from that point without the risk of an exchange rate fluctuation. The two-way peg would offer hosts a way to insulate themselves from the global monetary and credit markets'

CONCLUSION

Wiz is an improved variation of the Bitcoin protocol that allows cryptographic file encryption. Storage contracts may be used to ensure that clients store all the necessary information requested by the hosts. To guarantee access to storage, a host must have evidence of storage periodically. Whatever happens to the file on the host, the recipient would be charged. It is essential to point out that contracts do not compel the host to return any files as required. To reward hosts, rather than requesting that they provide and consume, it must establish a separate environment outside the network. It is often essential for clients and hosts to communicate in any way. One method is the block area, however. There are various safeguards mentioned which reduce the likelihood of Sybil attacks and host unreliability. Wiz provides the primary funding for Nebulous Inc., which is the organization that funds and releases, and maintains Wiz. The manner that Nebulous manages its crypto-currency funds explicitly contributes to the network's use and is not motivated by wrong parties' money, cheating the market of the currency. Other miners could even receive a block subsidy from Wiz money contributed to the project, with a similar result. We expect to provide pegs that enable customers to hedge themselves against fluctuations in the currency for the long term. We think Wiz is ideal for cloud storage that doesn't rely on confidence.