TAKE ME OUT TO THE BLOCKCHAIN

VOATZ, INC.
voatz.com

(To the tune of *Take Me Out to the Ball Game*.)

Take me out to the blockchain,
Take me out to the cloud.
Buy me some peanuts and smart contracts.
Distributed ledgers always have our backs.

1. THE FIRST PITCH: WHY SHOULD I CARE?

Learning about a new technology is exciting for some, but overwhelming for others. Wherever you are on that spectrum, our goal is for this paper to be a fun and thought-provoking overview of distributed ledger technology (also called blockchain technology), especially if you enjoy baseball.

Before we explain how the technology works, we will help you understand the motivation behind its development. Distributed ledger technology actually began in the early 1980s with David Chaum's Ph.D. dissertation, *Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups*.

The questions that Chaum posed and answered are relevant today. How do parties agree, despite potential mutual distrust? What if an arbiter or central authority is distrusted? Can we replace human arbiters, authorities, and procedures with mathematical protocols?

In the 1990s, Stuart Haber and Scott Stornetta asked related questions. How do you ensure the integrity and resilience of digital records? How do you prevent alterations to file time-stamps? Their work led to the first known blockchain, recorded in every Sunday edition of the *New York Times*.

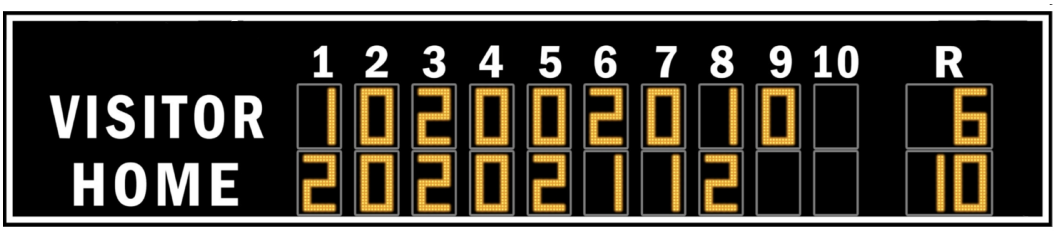
This was decades before the technology was applied to create Bitcoin.

The basic function of a distributed ledger is to store data, like a traditional database. The difference is in the way the data is structured, and is designed to resolve the questions posed by Chaum, Haber, and Stornetta.

For further study, we encourage you to take the free on-demand Blockchain Foundations[1] course by the GBA, but we will take a tour through a baseball game to explain the technology.

[1] https://gbaglobal.org/courses/blockchain-foundations/ (Government Blockchain Association)

2. EXPLAIN DISTRIBUTED LEDGER TECHNOLOGY TO ME LIKE I'M AT A BASEBALL GAME



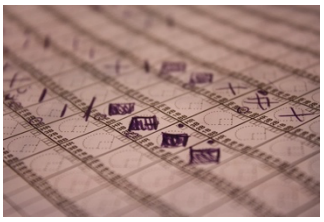
How can we be certain of the final score of a baseball game? That sounds like a silly question. Almost everyone who watches the game keeps track of the score. That's exactly how distributed ledger technology works. Let's unpack this concept.

Baseball games are divided into *innings* – 9 innings for professional baseball, with extra innings until a tie is broken. The scoreboard has a **block** of score data for each inning. Likewise, a distributed ledger consists of discrete blocks of data. These ledgers each have a "first inning" called a **genesis block**.

A baseball game follows the sport's codified **rulebook**. Every baseball team agrees to play by this rulebook. In the same way, distributed ledgers have a fixed set of codified rules that govern access to the data and the format of the data that it stores. A computer program, called a **smart contract**, can be stored on a blockchain and is triggered when certain conditions are met. By analogy, many baseball stadiums have certain traditions to start the seventh inning stretch.

During a baseball game, there are many **observers** who all agree on changes to the score each time a run is scored. In the same way, data stored in a distributed ledger is observed and validated by every server (**node**) in the ledger's network. Software on these nodes is designed to distinguish data that should be stored in the ledger from invalid data and invalid requests.

The observers include players, coaches, umpires, spectators, and fans watching on TV. These observers are **distributed** geographically and the scoreboard is transmitted publicly and globally via internet, TV, and radio. Likewise, data in the ledger is sent to each node on the network for validation. Depending on the rules governing the ledger, access to read the data on the ledger can either be public or restricted.



Each run is recorded on the scoreboard in the current inning, and the run total is also updated. This anchors each run to a specific inning. Since the innings are sequential, each run is fixed within a relative span of time. Runs are **timestamped**. In the same way, data stored in a distributed ledger is fixed to a moment in time, in a single block, between the blocks that were created before and after it.

Once a run is scored, that run cannot be erased. A team cannot go back in time to a previous inning to record more runs. In other words, inning run totals are **immutable**. In the same way, data recorded in a block on a blockchain cannot be altered.

At the end of the baseball game, the scoreboard is the arbiter of truth. The final score is confirmed by all observers, so everyone agrees with the score and the winner. Likewise, all who observe data on a blockchain can agree on the data, providing independent validation.

To summarize this analogy, a baseball scoreboard is a distributed ledger (blockchain). Inning run totals are blocks of data, connected in a chronological sequence, and it is impossible to go back and change the score. Game action and score data are simultaneously distributed, observed, and validated by spectators, players, coaches, and officials, resulting in **consensus** of the data.

3. SCORE SOME RUNS: HOW DISTRIBUTED LEDGERS CAN HELP YOUR STATE OR TERRITORY.

There are numerous applications of distributed ledger technology across various industries. Here are a couple relevant ideas in which it shows promise to provide substantial benefit.

3.1. VOTER REGISTRATION

What is the registration dilemma? How do you verify and maintain voter registration records efficiently, especially when voters move? Both Crosscheck and ERIC (Electronic Registration Information Center) have offered an answer to this question. However, Crosscheck was suspended in 2019 over concerns about data security and the privacy of personal information. Nine states have recently withdrawn from ERIC over data transparency concerns. What kind of alternative solution could assuage these concerns?

A national distributed ledger infrastructure could enable all U.S. citizens to have a **self-sovereign**[2] digital voter registration record on a blockchain, allowing them to verify their identity and confirm that their information stored on the chain is correct. Running a pilot of this concept across a single state, territory, county, or city could be a practical first step.

There are some questions, though, that naturally arise.

If data on a blockchain is immutable, how is voter registration information updated? One way to accomplish this is to create a new record on the chain with a link to the old record. This would establish an immutable record of changes to a citizen's record.

How do you protect a citizen's privacy and security if their registration data is recorded on a ledger? Sensitive data must be **encrypted**[3] so that only the citizen and authorized officials can read it, utilizing virtual identifiers instead of actual data.

Accurate voter registration records will help mitigate many of the issues reported in elections over the past several years. A blockchain-based solution will also satisfy the growing demand for transparency.

[2] The citizen has complete control over what personal information is stored and what information is shared with others.
[3] Encrypted data is mathematically scrambled so that only the intended recipient(s) can read the data.

3.2. VOTING

In May, the country of Turkey held elections for President. Officially, the incumbent won the election with about 52% of the vote, but his main opponent disputed the results. Are his claims true? Could such a disagreement be prevented in the future?

Could a distributed ledger infrastructure satisfy the growing demand for transparency in elections? Just as a baseball scoreboard displays results that are indisputable to the public, a distributed ledger could record ballot data and track vote totals for any election. Indisputable results could be announced quite quickly.

There are a couple obvious questions. We have thought of them.

How do you prevent the release of vote tallies until an election closes? Just as one would encrypt sensitive voter registration data, ballot data and tallies would be encrypted until the election closes. Yes, there are ways to tally encrypted ballots without decrypting them. The technical term for this is **homomorphic encryption**.

What about paper ballots? We invite you to read the GBA Remote Election Technology Report and our 2022 Winter NASS whitepaper linked below. The latter suggests hybrid approaches to digitize elections while maintaining an official paper ballot record.

4. THE FINAL OUT: WRAP-UP

Various individuals and organizations contend that blockchains are not appropriate for public elections. Once we understand how distributed ledgers work and what questions they resolve, do their arguments withstand objective reasoning?

Distributed ledger technology can establish and prove trust between government and the people by replacing human and “black box” operations with publicly verifiable data, stored in chronological blocks of data. Distributed ledger technology is an unbiased and independent arbiter of truth.

5. EXTRA INNINGS: MORE INFORMATION

1. GBA: gbaglobal.org: The Government Blockchain Association connects people and organizations with blockchain-based solutions to problems typically faced by government entities.

2. Remote Election Technology Report, GBA: https://gbaglobal.org/wp-content/uploads/2023/06/2022-07-29-Remote-Election-Tech-Report-Final2.pdf

3. Parallel Internet and Paper Elections: A Practical PIPEline to Secure and Accessible Elections: https://www.nass.org/sites/default/files/2022-02/Voatz-white-paper-nass-winter-2022.pdf