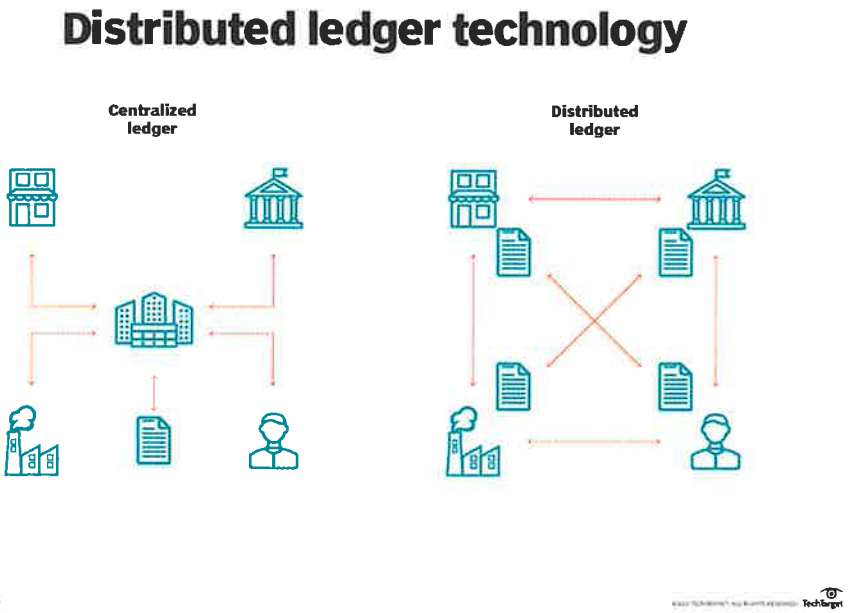
SIMPLIFYING CRYPTO PROJECTS

An (Oversimplified) Introduction to Key Concepts

THE MAIN CONCEPT



- Crypto projects are fundamentally just databases (ledgers).
- The big deal is that the databases are distributed…
- …and read/write access (authentication) is controlled by algorithm…
- …over a network of computers (nodes).

WHY IT MATTERS

- The (observable) algorithms replace a "trusted manager."
- This allows individuals to share access to information…
- …even though they may not trust each other…
- …but still trust that the information is accurate.

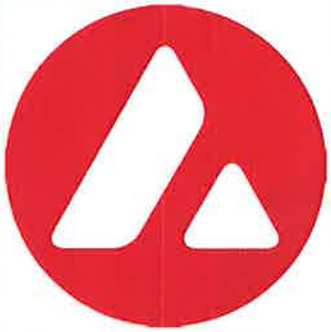
WHY THAT'S USEFUL & WHEN IT'S NOT

- Cartels need to cooperate while competing
- Groups of individuals want to share some parts of a dataset, while keeping others private
- Groups of individuals can't trust a single arbiter of information

- Everybody trusts the database manager
- Speed and efficiency of access are top priorities
- There is one proprietary "owner" of the information

THE KILLER APP IS MONEY, BUT....

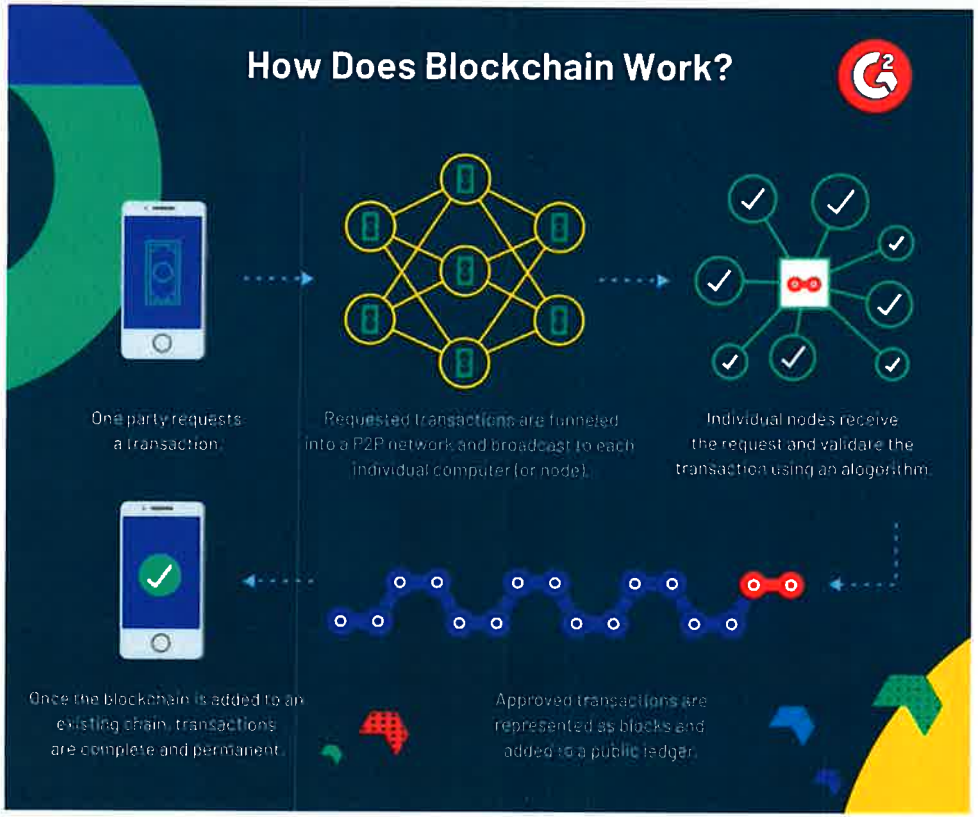
...THERE ARE MORE NON-MONEY USES



MANY TYPES OF DISTRIBUTED LEGDERS

- Blockchains
- Directed Acyclic Graphs (DAGs)
- Holochains
- Hashgraphs

BLOCKCHAINS ARE THE MOST POPULAR



THE "CRYPTO" PART

- Public/Private Key Cryptography secures the data, and
- Cryptographic Trapdoor (Hash) Functions compress data, allow for data verification, and level the computing playing field…
- …which allow the algorithms to replace a "trusted manager" by…
- …creating "proof" conditions for network computers (nodes).

PROVE WORK OR PROVE HOLDINGS

Proof of Work (POW)

- Amount of work determines read/write privilege
- Game theory conditions incentivize a higher level of network security
- Resource/energy intensive

Proof of Stake (POS)

- Amount of holdings determines read/write privilege
- Low resource/energy usage
- The "rich" have greater defacto network control

POW -VS- POS

- POW is generally better for monetary applications
- POS is generally better for non-monetary applications
- Differential energy rate charging will incentivize POS algorithms