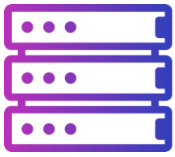

DBGrow

Projects

Version: 1.0

Introduction

The following document details DBGrow's current projects, and some of our future interests.

4. Current Projects

4.1 Factom Dapps Framework

DBGrow has achieved a proof of concept for the deployment and execution of smart contracts and DApps on top of Factom. Although Factom Inc. CEO Paul Snow has hinted at the idea of Factom supporting smart contracts, this has yet to be achieved in practice until now. DBGrow is very excited to spearhead achieving this goal.

Pre-Alpha: Factom Dapps

4.2 Factom ObjectDB

Written in NodeJS, this project allows developers to store and track changes to JSON objects using Factom. This opens up many possibilities for Factom's use as a general purpose decentralized data layer. Objects may be publicly readable or private (encrypted), and can be easily verified for authenticity.

Pre-Alpha: Factom ObjectDB

4.3 Factom-MongoDB-node Library

We have begun development of a NodeJS library that utilizes Factom ObjectDB to create immutable audit trails for MongoDB databases. The library tracks changes to objects in real time via the database's Oplog, and secures them to the Factom blockchain.

Pre-Alpha: Factom Mongodb Node

4.4 Cloud Provider Quick-Start Guide + Images

DBGrow has developed and released a quick-start guide and set of VM Images for teaching new Factom users best practices for deploying a Factom Testnet node on popular cloud providers. Our VM Images make it quick and easy to get started running a testnet node, and include a pre-synced copy of the Factom Testnet blockchain. The first release of the guide is compatible with AWS. Soon, we will also support other popular providers like Microsoft Azure, Google Cloud Platform, and DigitalOcean.

If the community finds this project beneficial, we will also begin publishing daily backups of the Factom testnet and mainnet blockchain to make provisioning new hosts and recovering from disasters as fast as possible.

AWS Full release: Factom Testnet Cloud Guide + Images

4.5 Support Application + Proof of Support

DBGrow's has been developing a "proof of support" application to enable server operators to demonstrate their provision of 24/7 support. This application will be made available to the broader community upon completion.

See Proof of Support Application supplemental document for more information on this topic.

4.6 Promoting Factom

We will reach out to to new users and organizations as an integral part of our mission to further the Factom protocol. So far, the DBGrow team has sought out and had informal discussions with a multitude of people spanning corporate and scientific domains. We most recently made contact with a Ford Motor Company blockchain researcher, and reached out to informally discuss their work and the potential applications of Factom. The engagement and interest we have seen throughout these conversations on the role systems like Factom could play in their work has been very exciting. We will actively

seek to leverage our ties within several prominent Silicon Valley technology conferences, meetups, and Bay Area hackathons to promote Factom through featured talks and tabling events.

5. Future Projects

5.1 Factom Wiki

The DBGrow team believes that an accurate, concise, and easy to access information source for Factom will help increase adoption, decrease misinformation, and save developers time. For that reason we plan to organize and develop a series of Factom tutorials and compile answers to important technical questions we see repeated in the community. We want the Factom Wiki to be a community maintained resource that is useful for both new adopters and veterans.

We have obtained the following domain to host this project: FactomWiki.org

5.2 Scientific Applications

Our team has built connections at research institutions around the bay area including LBNL (Lawrence Berkeley National Laboratory), NASA Ames, UC Davis, and UC Berkeley. Two of our team members have experience working in materials and biophysics research labs, and one is currently a researcher at LBNL. Due to these factors, we are well positioned to explore the applications of Factom for scientific research. We aim to be an interface for the Factom community to access feedback, ideas, and test applications with the world of scientific research.

One application we believe Factom is well suited for is securing real-time data from scientific and industrial equipment. This includes High Performance Liquid Chromatography (HPLC), Mass Spectrometry (MS), and other analytical instruments used for quality control and monitoring across many industries. A major component of most commercial HPLC and MS software are modes of operation that aim to ensure data integrity and prevent manipulation of results. Currently, the available software is proprietary, costly, and less secure and immutable than what we believe can be built by securing results with Factom. In many countries there are laws requiring validation of

quality control data, as seen in the following U.S Food and Drug Administration (FDA) warning letter to Sunrise Pharmaceutical:

> 6. Your firm has not exercised appropriate controls over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel [21 CFR 211.68(b)]. For example, your firm lacks systems to ensure that all electronic data generated in your Quality Control laboratory is secure and remains unaltered … In addition, your firm's review of laboratory data does not include a review of an audit trail or revision history to determine if unapproved changes have been made … Further, your response does not address security procedures to ensure that the data generated using the new HPLC units is secure and remains unaltered. (Amador-Toro, 2010)[1]

Leveraging Factom for an end to end solution that secures this testing data in real time would directly address the problems the FDA is presenting here. This application is only the beginning of the role Factom could play in laboratory and industrial settings. We want to further explore the role Factom can play in addressing issues like P-hacking, and making provable scientific data easier to share. This will be a long term project, but we have already started to garner interest for such an application. Firstly, we would work on implementing software on top of instruments in our possession such as HPLC machines, and would ultimately like to submit a proposal to LBNL to test such a system in the laboratory in which our team member works.

5.3 Public Key Infrastructure

We are interested in exploring a Factom-based public key infrastructure solution with greater transparency, security and affordability compared to current systems to authenticate public keys for digital signatures and encryption.

Currently, the dominating approach to public key infrastructure relies on a third-party Certificate Authority (CA) who is responsible for issuing certificates to public key holders (such as servers hosting secure websites) and then subsequently verifying to other parties (such as web browsers) that the key is correct.

Currently roughly 85% of the CA marketshare is held by only three companies[2]. Breaches can go unnoticed for long periods of time, and the public must trust the CA to identify and disclose breaches. Entities must trust that the CA has not been hacked[3] or ordered to issue fraudulent certificates allowing intelligence agencies to masquerade as a website or other service[4]. Existing distributed alternatives to CA's such as the PGP based Web of Trust have infrastructure scaling and security problems and have seen

limited adoption. We believe Factom can be leveraged to create a public key infrastructure akin to a Factom secured Web of Trust.

5.3 Warrant Canaries

We are interested in exploring the application of Factom to maximize the utility of warrant canaries. Using Factom's immutability and ability to prove a chain's lifetime, we aim to create a warrant canary system that secures the entity's specific attestation while preventing another entity from pointing to a new stream of forged attestations. Methods such as warrant canaries have been used by companies and other organizations to be transparent to the public about their interactions with the government by leveraging their legal protection against being forced to make a false statement regarding an interaction, regardless of a gag order prohibiting the company from specifically divulging an interaction.