History

In 2013, the Bitcoin network experienced tremendous growth, which inspired many people. At the time, DFINITY Foundation founder Dominic Williams was running an MMO (https://en.wikipedia.org/wiki/Massively_multiplayer_online_game) computer game he had built and grown to several million users, in the role of an engineering entrepreneur, using custom technical infrastructure. He caught the Bitcoin bug like many others, and having already worked extensively with cryptography and distributed systems, he transitioned to working full-time in blockchain.

By the end of 2013, Dominic was seeking technical means to build faster blockchains that could process more transactions per second, which he hoped would support a trade in virtual goods within the computer games ecosystem, and he acquired the domain name "gamecoin.org." This activity led to him spending 2014 working on a blockchain project called "Pebble." His work on Pebble pioneered two major firsts in blockchain: (1) the adaptation of traditional distributed computing mathematical techniques for use within a blockchain setting, and (2) an effort to design a scalable blockchain that could process hundreds of thousands of transactions a second.

The Internet Computer

Dominic released v0.977 of the Pebble white paper in October 2014. Although it represented the product of substantial work, at 98 pages in length, at the time it was only circulated among early crypto industry insiders, and cryptographers, including Vitalik Buterin, Nick Szabo, Elaine Shi and Dan Boneh. The project had great potential, and propounded several important new approaches to blockchain design, but was ultimately not pursued, largely owing to Dominic's emerging interests as part of the early Ethereum community.

While working on Pebble in 2014, Dominic had become involved with the early Ethereum community, becoming an avid early supporter of the project, which he remains to this day. At the time, the concept of a blockchain that could run software (i.e. smart contracts), which stored and processed data within an unstoppable, tamperproof and autonomous on-chain environment, was both revolutionary and controversial within the industry. Ethereum was pioneering a new "general-purpose" form of blockchain, which departed from "coins-only" designs, such as Pebble. This upset some parts of the Bitcoin community. Vitalik Buterin (https://en.wikipedia.org/wiki/Vitalik_Buterin), the founder of Ethereum, credits Dominic with co-inventing the term "Bitcoin Maximalism" (https://twitter.com/VitalikButerin/status/987360195553759232) during this era.

At some point, the concept of a blockchain playing the role of a "World Computer" was mooted within the Ethereum community. One interpretation was that such a network would perform a trickle of simple but important smart contract computations for the world. However, Dominic's interpretation, based on his work, was that World Computer blockchain would inevitably eventually host much of humanity's systems and services, and all its data and compute, largely replacing traditional IT, and transforming social media, gaming, finance, enterprise systems and many other domains.

In 2015, however, Dominic was a lone heretic, and was largely alone in believing that the creation of a true World Computer blockchain was technically feasible, let alone that it might be capable of successfully playing that role in competition with centralized computing infrastructure. Since Dominic strongly believed otherwise, based on his accumulated technical experiences and work on crypto theory, he decided to dedicate himself to blockchain research that might realize the concept, originally, he hoped, in the form a more advanced Ethereum 2.0. He stopped work on Pebble, and directed all his future efforts towards the realization of the World Computer blockchain vision.

In early 2015, Dominic's thinking about blockchain design had become more mature, and he began proposing new approaches to consensus, applied cryptography and blockchain network architecture. Around that time, he began using the name DFINITY as a brand for his work, which takes its characters from **d**ecentralized in**finity**. During this era, Dominic was pioneering multiple technical approaches that have been proven over time, and innovations that remain powerful ideas today. Much of his early 2015 work was also targeted towards improving the performance and scalability of existing Proof-of-Work networks like Bitcoin.

Here in May 2015 Dominic gives a talk discussing Sybil resistance and consensus at San Francisco Bitcoin Devs (https://www.youtube.com/watch?v=dfGDhDR_3Gc), in which he describes the "3 E's of Sybil Resistance" and discusses consensus work originating from the Pebble project. Other interesting historical material that provides insights into his role at the time, include a panel on scalability with Vitalik Buterin and Gavin Wood (https://www.youtube.com/watch?v=1KaQsrqC94s), and a talk introducing basic aspects of consensus theory (https://www.youtube.com/watch?v=3iSw03pJ-gk), at Ethereum's DEVCON1 later that year.

Through the period 2015 to 2016, Vitalik Buterin, and associates such as Vlad Zamfir, were the Ethereum project's primary consensus researchers, and were highly focused on developing cryptoeconomic (https://en.wikipedia.org/wiki/Cryptoeconomics) schemes, including under the Casper banner. Meanwhile, Dominic was more focused on finding new ways to leverage advanced cryptography and distributed computing math, and devising alternative blockchain architectures, which might enable a World Computer to be produced. Owing to the long-term nature of Dominic's work, and its more technical approach, eventually it became clear to him that DFINITY should become an independent project.

Although the DFINITY project eventually trod its own longer path, important traces of DFINITY thinking remain within the Ethereum project. For example, early in 2015, Dominic first proposed using a scheme called Threshold Relay, which involved using BLS cryptography (https://en.wikipedia.org/wiki/BLS_digital_signature) to generate random numbers, then using those numbers to drive a blockchain — essentially by selecting random committees of nodes that would produce and finalize blocks by "attesting" to, or "witnessing" them. Ethereum 2.0's Beacon Chain (https://ethereum.org/en/upgrades/beacon-chain/) is partly a realization of that 2015 concept.

Dominic's own work at DFINITY also had many important antecedents. For example, he himself became interested in the idea of using cryptography to generate random numbers in a network and using them to drive consensus after reading the Random Oracles in Constantinople: Practical Asynchronous Byzantine Agreement using Cryptography (https://allquantor.at/blockchainbib/pdf/cachin2000random.pdf) research paper, among others, in 2014. One of the authors of this paper, famous cryptographer and distributed computing scientist Victor Shoup (https://www.shoup.net/), later joined the DFINITY Foundation in 2021.

Early in 2015, Dominic's Threshold Relay scheme was redesigned to use BLS threshold cryptography (https://en.wikipedia.org/wiki/BLS_digital_signature) to generate random numbers. This was thanks to a meeting with famous cryptographer Dan Boneh (https://crypto.stanford.edu/~dabo/) at Stanford University, which was near to where he lived at the time in Palo Alto, California. Dan Boneh is the B in "BLS," and later, early in 2017, the DFINITY Foundation hired Ben Lynn (https://crypto.stanford.edu/~blynn/) from Google, who was the "L".

For some years after Dominic began promoting his Threshold Relay system for producing random numbers in a decentralized setting, in a way that is unmanipulable, unpredictable, and unstoppable, using BLS threshold cryptography, Vitalik Buterin raised concerns about the safety of using BLS. A fun back and forth on the subject at a Silicon Valley Ethereum meetup (https://youtu.be/h2pONw0eTTk?t=1707) in late 2016 reflects the congenial and collegiate back and forth that was characteristic in the community at the time. Vitalik eventually became convinced about the safety of BLS, and Ethereum 2.0 now relies on BLS.

The complexity of Dominic's early technical designs, and general disbelief about the viability of building a World Computer blockchain, made it hard for him to muster support for his ideas, and persuade the Ethereum community to work on implementations. However, in 2016, Dominic was co-founder of a crypto incubator called String Labs. After a DeFi project to produce "mirror assets" was complicated by regulatory concerns, Dominic persuaded co-founder Tom Ding that String Labs should instead incubate DFINITY, and help it become a standalone project. String Labs was primarily backed by Chinese venture capital, which also played a crucial early role in the early years of the Ethereum ecosystem.

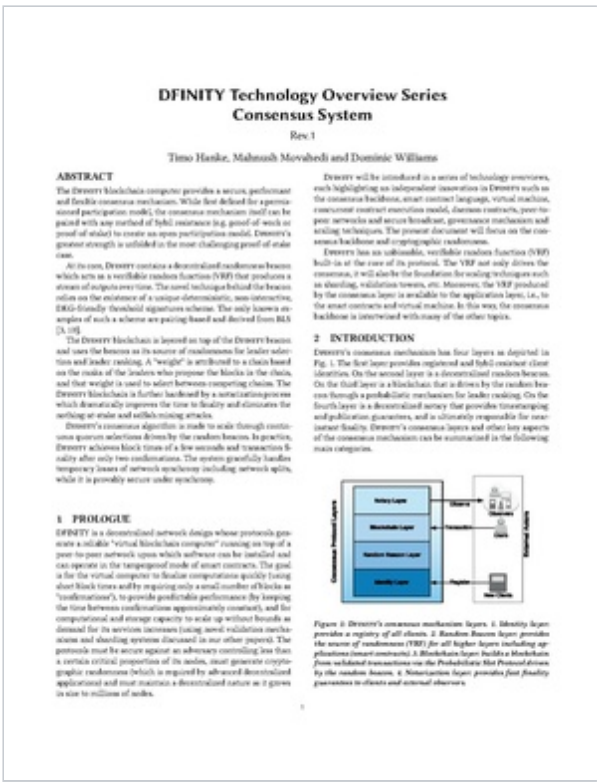
At this time, they were joined by Timo Hanke, the developer of AsicBoost (https://decentralpost.com/asicboost/), and the CTO of CoinTerra, from the Bitcoin community, and other people. Dominic decided to follow the fundraising example provided by Ethereum, and create a neutral not-for-profit foundation to drive development of a World Computer blockchain protocol. Accordingly, the DFINITY Foundation was formed in Zug, Switzerland, with Dominic as President, in October 2016, later moving to Zürich, Switzerland, when it established a large research center there.

To bootstrap the ecosystem, the ICP token ledger was created using smart contracts on the Ethereum network in January 2017, which included allotments for early contributors, and an endowment for the DFINITY Foundation. A seed donation was then run February 2017, which allocated ICP (then called DFN) to the public on behalf of the DFINITY Foundation, to raise funding for its work.

In the February 2017 Seed donation round, ICP was allocated to Seed donors in exchange for donations of bitcoin (BTC) and ether (ETH), which was marked-to-market, such that a contribution of 1 Swiss franc was rewarded by 30 ICP. This meant that hundreds of members of the public were allocated ICP at approximately 3 cents each. Through this seed donation, the DFINITY Foundation received $3.9 million in initial funding, although total cash receipts were greater, as the value of the ETH and BTC received increased substantially before it was sold by the foundation.

This initial funding allowed the foundation to begin expanding its operations. Notable early technical hires included Ben Lynn, and Andreas Rossberg (https://people.mpi-sws.org/~rossberg/), also from Google, who was the co-inventor of WebAssembly. They were also joined by Artia Moghbel (https://www.linkedin.com/in/artiam/) heading up operations, who previously worked for a VC that had invested into the MMO game Dominic had earlier developed. By October 2017, Dominic was able to demonstrate an initial version of its test network (https://www.youtube.com/watch?v=aOzxxeOYJpY) to the world, which included an implementation of Threshold Relay, and a basic version of Probabilistic Slot Consensus, together with a novel smart contract execution environment, and a smart contract language derived from Haskell, for the first time.

In January 2018, DFINITY published its first formal white paper describing its consensus system, although it had been described informally for some time. With this, and the test network in hand, the DFINITY Foundation decided to raise significant additional funds and scale-out its operations — since it the scope of the R&D work required to deliver a true World Computer was substantially broader than originally anticipated.


DFINITY Technology Overview Series
Consensus System
Rev.1
Timo Hanke, Mahnush Movahedi and Dominic Williams
ABSTRACT
1 PROLOGUE
2 INTRODUCTION
2018 DFINITY Foundation white paper describing its consensus system.

The DFINITY Foundation raised more than one hundred millions dollars in two fundraising rounds in 2018, the Strategic Round and the Presale Round. This enabled it to scale its operations more aggressively. The major challenge was building out an R&D organization that could effectively combine blue sky computer science and cryptography research activity, with engineering operations. In practice, this was a process that took many years, and many bumps on the road were passed en route to the organization as it is today.

In 2018, the DFINITY Foundation's CTO (Chief Technology Officer), Jan Camenisch (https://jan.camenisch.org/), a famous cryptographer, was hired from IBM, where he worked as a Principal Research Staff Member. He became instrumental in building out the Zürich research center. This included recruiting numerous well-known cryptographers to the World Computer mission, whom he had often worked with before. Arguably, the DFINITY Foundation employs more well-known and highly respected cryptographers than any other organization in the tech industry. This is in sharp contrast to other blockchain projects, which often do not employ any cryptographers at all, preventing them developing custom cryptography to meet their needs.

Collectively, DFINITY Foundation cryptographers, researchers and engineers have published more than 1500 papers, collected more than 88,000 citations, and have created more than 190 patents. As the Zürich research center grew, it became the largest employer of ex-Googlers in Switzerland, with many joining from Google Research. Across all research centers, including California, more than 20% of all staff members joined from Google or IBM, and more than 20% are alumni of Zürich ETH and EPFL. The DFINITY Foundation has a better balance of the sexes than most tech organizations, and 43% of department heads across the world are women.

To launch the Internet Computer, the R&D team had to implement protocols that would allow it to establish chain key cryptography material on nodes in a decentralized network setting. This was achieved using a groundbreaking non-interactive DKG (distributed key generation) and key re-sharing protocol, devised by Jens Groth (http://www0.cs.ucl.ac.uk/staff/j.groth/), another famous cryptographer working at DFINITY. This works in conjunction with updated protocols, described in "The Internet Computer for Geeks" paper.

The scale of the technical challenges involved in creating a protocol that incorporated such advanced cryptography and protocol math was enormous, and was achieved only through the incredible efforts of a large and highly dedicated team of cryptographers, computer science researchers and engineers. The Internet Computer also uses a completely novel blockchain architecture, which is necessary to deliver the World Computer vision, and depends on many innovations in areas spanning its WebAssembly-based smart contract execution environment to new computer languages such as Motoko. The Internet Computer network is also adaptive, self-governing and self-updating, thanks to an advanced DAO called the Network Nervous System that runs within its protocols. It represents an enormous technical achievement.

The Internet Computer runs on a sovereign network of special node machines, which is dedicated hardware. Before its May 2021 genesis event and production network launch, a community of independent node providers had to be established, who would purchase or build these machines, and run them from data centers around the world. This was bootstrapped by the DFINITY Foundation.

The Internet Computer network underwent genesis May 2021, and transitioned into a decentralized production mode. This will be seen as an momentously impactful event in the history of tech and blockchain. Nonetheless, at launch, the Internet Computer project faced a firestorm of attacks from other projects in the blockchain industry, who feared its capabilities. The DFINITY Foundation, which is primarily a research and development organization, was ill-equipped to deal with the attacks, and was substantially disrupted for some time. The full scale of the attacks and corruption directed at the project is now slowly being exposed, including by investigative journalism efforts such as https://cryptoleaks.info.

The attacks that were launched also substantially disrupted the markets for the Internet Computer network's ICP utility token, and led to misconceptions and disinformation about the project becoming widespread. Thankfully, this situation is slowly clearing, and moreover, it did little to dent developer interest in the project.

The Internet Computer community is fast growing and strong. There are now thousands of developers building on the Internet Computer network, and thousands of web3 and other projects running. Indeed, its developer community regularly clocks more "GitHub commits" than any other in the blockchain industry. Projects running on the Internet Computer are unique in the blockchain industry, because they run entirely from the blockchain, without reliance on cloud computing and centralized traditional IT to function, as is required with other blockchains. Smart contracts running on the Internet Computer can create transactions on other blockchains, and its capabilities are now being used to orchestrate multi-chain systems, and create user experiences and functionality for services running on other chains.


Non-interactive distributed key generation and key resharing

Jens Groth[1]

jens@dfinity.org
DFINITY Foundation

Draft
March 16, 2021

Abstract. We present a non-interactive publicly verifiable secret sharing scheme where a dealer can construct a Shamir secret sharing of a field element and confidentially yet verifiably distribute shares to multiple receivers. We also develop a non-interactive publicly verifiable resharing scheme where existing share holders of a Shamir secret sharing can create a new Shamir secret sharing of the same secret and distribute it to a set of receivers in a confidential, yet verifiable manner.
A public key may be associated with the secret being shared in the form of a group element raised to the secret field element. We use our verifiable secret sharing scheme to construct a non-interactive distributed key generation protocol that creates such a public key together with a secret sharing of the discrete logarithm. We also construct a non-interactive distributed resharing protocol that preserves the public key but creates a fresh secret sharing of the secret key and hands it to a set of receivers, which may or may not overlap with the original set of share holders.
Our protocols build on a new pairing-based CCA-secure publickey encryption scheme with forward secrecy. As a consequence our protocols can use static public keys for participants but still provide compromise protection. The scheme uses classical encryption, which comes at a cost, but the cost is offset by a saving gained by our ciphertexts being comprised only of source group elements and no target group elements. A further efficiency saving is obtained in our protocols by extending our single-receiver encryption scheme to a multi-receiver encryption scheme, where the ciphertext is up to a factor 3 smaller than just having single-receiver ciphertexts.
The non-interactive key management protocols are deployed on the Internet Computer to facilitate the use of threshold ECS signatures. The protocols provide a simple interface to remotely create secret-shared keys to a set of receivers, to refresh the secret sharing whenever there is a change of key holders, and provide proactive security against mobile adversaries.

1 Introduction

The Internet Computer hosts clusters of nodes running subnets (shards) that host finite state machines known as canisters (advanced smart contracts). The

2021 Dfinity Foundation paper, non-interactive distributed key generation and key resharing


The Internet Computer for Geeks

(v1.3)

The DFINITY Team*

April 19, 2022

Abstract

Smart contracts are a new form of software that will revolutionize how software is written, IT systems are maintained, and applications and whole businesses are built. Smart contracts are composable and autonomous pieces of software that run on decentralized blockchains, which makes them tamperproof and unstoppable. In this paper, we describe the Internet Computer (IC), which is a radical new design of blockchain that unleashes the full potential of smart contracts, overcoming the limitations of smart contracts on traditional blockchains with respect to speed, storage costs, and computational capacity. This allows smart contracts for the first time to implement fully decentralized applications that are hosted end to end on blockchain. The IC consists of a set of cryptographic protocols that connects independently operated nodes into a collection of blockchains. These blockchains host and execute "canisters", the IC's form of smart contracts. Canisters can store data, perform very general computations on that data, and provide a complete technology stack, serving web pages directly to end users. Computational and storage costs are covered by a "reverse-gas model", where canister developers pre-pay costs in cycles that are obtained from ICP, the native token of the IC. ICP tokens are also used for governance: the IC is governed by a decentralized autonomous organization, or DAO, which, among other things, determines changes to the topology of the network and upgrades to the protocol.

1 Introduction

1.1 Unleashing smart contracts

Because of their unique features, smart contracts are the key enabler of Web3, the new approach to the web where applications are fully controlled by their users and run on decentralized blockchain platforms. Such decentralized applications (dapps) are typically tokenized, meaning tokens are distributed to users as rewards for participating in the dapps. Participation can come in many different forms, ranging from moderating and providing content to governing a dapp and to creating and maintaining a dapp. Usually, tokens can also be bought on exchanges; indeed, selling tokens is a common way to finance dapp development. Finally, tokens are also used as a form of payment for the services or contents a dapp offers. Smart contracts running on today's blockchain platforms, including all the

*https://dfinity.org/foundation/; contact author: Victor Shoup, victor.shoup@dfinity.org.

1

2022 DFINITY Foundation paper, "The Internet Computer for Geeks"

The DFINITY Foundation, and the fast growing Internet Computer community, are focused on building-out a new web3 internet ecosystem, and eventually moving the vast majority of online systems and services onto the Internet Computer, in a replacement of traditional IT that drives a blockchain singularity.