

Curriculum Vitae of James (Jim) McDonald

Jim.McDonald@wealdtech.com

England, United Kingdom

Experience

Attestant Limited

Chief Technology Officer, Co-founder

2019 – Present

Co-founded Attestant, a company focused on Ethereum staking. Heavily involved with the design of the initial architecture, Attestant is recognized as the gold standard staking service for Ethereum.

Frequently participating in the specifications process of the Ethereum protocol and working across multiple client teams to ensure that specifications are both robust and able to be implemented in the real world.

Designed and built the preeminent distributed signing system used for Ethereum validators, named Dirk, as well as the only multi-node validator, called Vouch. Vouch and Dirk, as well as their constituent components, are used in a number of the Ethereum clients and in many competing staking services.

Generating the majority of the company's articles and much of its marketing copy, balancing the technical features of the product with Attestant's customer focus to ensure high customer acquisition and retention rate. Presenting at conferences and directly with customers in sales calls, covering the product, the company ethos, and why Attestant deserves its moniker as the premium Ethereum staking service.

Contributing to a large number of open source projects to improve and enhance user and staker experience on Ethereum.

Weald Technology

Managing Director

2012 – Present

Managing director. Advisor to technology companies in the enterprise computing space and beyond. Early stage investor in companies ranging from regenerative biotechnology to fintech. Actively involved in a number of emerging technologies such as cryptocurrencies, and specifically Ethereum. Consulting in a range of capacities from corporate strategy to expert witness. Advising a number of firms in the cryptocurrency space.

Xiotech

Chief Strategy Officer

2009 - 2012

Tasked with reinvigorating Xiotech's products as well as increasing their company presence and product visibility. Worked across all divisions to streamline the company, reduce legacy business, and focus the company on a single product line.

Participated in company fund-raising by presenting the company, the technology, and the business plan to a range of technical and non-technical audiences.

Managed the internal production and external release of Hybrid ISE, Xiotech's first major product launch in three years, which was recognized as the first true hybrid SSD/HDD storage subsystem.

EMC

Chief Technology Officer, Storage Software Group

2008 - 2009

Integrated WysDM personnel and departments with EMC. Worked with sales and marketing to promote WysDM's presence to EMC's salesforce. Took the executive lead with some of EMC's largest customers.

WysDM Software

Chief Technology Officer, Co-founder

2002 – 2008

Co-founded WysDM Software, a firm providing management software for data protection technologies. Chief architect of the product suite and managing director of the UK arm of the company, the primary development location containing the majority of staff and expenditure. Provided high-level consultancy with large storage-related technology firms to ensure cash flow during initial product development.

Shifted focus after product release to sales, marketing, and business development. Became the executive presenter for worldwide events, customers and resellers, and technical lead for OEM partnerships. Authored white papers, sales material, etc. to support sales and marketing efforts.

Worked with analysts to define the data protection management space. Overcame multiple competitive products to become the market-leading data protection management solution in terms of revenue, market share, and installation base. Secured the business of both product and technology OEMs, most notably with EMC.

Managed a successful exit to EMC as a profitable company with a market-leading product, strong growth of top-line and bottom-line revenue, and a customer base including some of the largest financial, pharmaceutical, telecommunications and service provision companies in the world.

StorageNetworks

Director of Engineering

2000 - 2001

Managed a team of professionals that evaluated and deployed storage hardware and software. Visited a large number of customers and discussed their storage strategy and requirements. Acted as executive sponsor, which proved pivotal in securing a number of accounts.

Goldman Sachs

Systems engineer

1995 - 2000

Responsible for primary and secondary storage for the London office, systems, application monitoring for Europe, and storage engineering globally.

Education

BSc (Hons) Computer Science, University of Edinburgh (1995).

Selected Publications

Understanding withdrawals

Abstract: Understanding the process and mechanism of moving rewards from the consensus chain to the execution chain.

Publication date: 15th February, 2023

Link: <https://www.attestant.io/posts/understanding-withdrawals/>

Exploring the impact of MEV relays

Abstract: MEV relays have been introduced to the Ethereum network recently. This article looks at their impact on block times and chain stability.

Publication date: 23rd October, 2022

Link: <https://www.attestant.io/posts/exploring-the-impact-of-mev-relays/>

Exploring execution block rewards September 2022

Abstract: Compiling data about historical execution block rewards in an attempt to provide an expectation of future rewards.

Publication date: 5th September, 2022

Link: <https://www.attestant.io/posts/exploring-execution-block-rewards-sep-22/>

Understanding post-merge rewards

Abstract: The merge changes how rewards are issued to validators. This article examines different sources of rewards, and how they may be accessed.

Publication date: 31st March, 2022

Link: <https://www.attestant.io/posts/understanding-post-merge-rewards/>

Exploring execution block rewards

Abstract: Compiling data about historical execution block rewards in an attempt to provide an expectation of future rewards.

Publication date: 17th March, 2022

Link: <https://www.attestant.io/posts/exploring-execution-block-rewards/>

Evaluating beacon nodes 2022 edition

Abstract: An update of a previous article looking at the relative performance of beacon nodes in proposing blocks.

Publication date: 3rd March, 2022

Link: <https://www.attestant.io/posts/evaluating-beacon-nodes-2022/>

Helping client diversity

Abstract: Helping client diversity is not as simple as avoiding the majority client. This article explores how Vouch allows use of majority clients without the associated risk of finalizing an invalid chain.

Publication date: 15th February, 2022

Link: <https://www.attestant.io/posts/helping-client-diversity/>

Charting inactive Ether

Abstract: Ether on the beacon chain not actively participating in validating is a waste. This article charts the growth of inactive Ether in the first two weeks of the beacon chain.

Publication date: 21st January, 2021

Link: <https://www.attestant.io/posts/charting-inactive-ether/>

Exploring net issuance

Abstract: Net issuance on Ethereum 2 is a critical metric to understand total Ether supply. This article provides details on how to calculate its value.

Publication date: 14th January, 2021

Link: <https://www.attestant.io/posts/exploring-net-issuance/>

Examining Ethereum 2 network performance

Abstract: The Ethereum 2 network is a massively complex entity, but a single metric encompassing its performance is very useful. This article describes such a metric.

Publication date: 7th January, 2021

Link: <https://www.attestant.io/posts/examining-ethereum-2-network-performance/>

Introducing Vouch

Abstract: Attestant uses their own multi-node validator client, providing high levels of security and availability whilst fitting neatly in to production environments. This article introduces Vouch and explains its features.

Publication date: 28th September, 2020

Link: <https://www.attestant.io/posts/introducing-vouch/>

Evaluating beacon nodes

Abstract: Multiple implementations of the Ethereum 2 node software exist. This article compares some of them to see if one is significantly better than the others.

Publication date: 11th September, 2020

Link: <https://www.attestant.io/posts/evaluating-beacon-nodes/>

Introducing Dirk

Abstract: Attestant uses their own distributed remote keymanager, providing high levels of security and availability whilst fitting neatly in to production environments. This article introduces Dirk and explains its features.

Publication date: 25th August, 2020

Link: <https://www.attestant.io/posts/introducing-dirk/>

Defining attestation effectiveness

Abstract: Attestation effectiveness is a great metric to help understand how your validators are performing. This article explains what attestation effectiveness is, and how to calculate it.

Publication date: 6th August, 2020

Link: <https://www.attestant.io/posts/defining-attestation-effectiveness/>

Protecting validator keys

Abstract: Protecting validator keys is difficult due to their dual requirements of security and accessibility. This article discusses various methods to increase both security and accessibility of validator keys.

Publication date: 30th July, 2020

Link: <https://www.attestant.io/posts/protecting-validator-keys/>

Protecting withdrawal keys

Abstract: Protecting withdrawal keys is a critical part of any Ethereum 2 staker's operations. This article discusses the use of withdrawal keys and how they can be secured with existing tools.

Publication date: 11th June, 2020

Link: <https://www.attestant.io/posts/protecting-withdrawal-keys/>

Charting Ethereum issuance

Abstract: Ethereum 1 secures its chain using a proof of work consensus mechanism, whereas Ethereum 2 uses proof of stake. Both networks create Ether to reward participants, however this increases the total Ether supply. This article looks at the technical changes coming to the Ethereum 1 and Ethereum 2 networks that will result in both short-term and long-term changes to the total supply of Ether.

Publication date: 7th May, 2020

Link: <https://www.attestant.io/posts/charting-ethereum-issuance/>

Custodial staking in Ethereum 2

Abstract: Ethereum 2 staking is on the horizon and a great opportunity to put otherwise-dormant Ether to work. A number of exchanges and custodians have announced they will start providing interest on Ether held in custody. Is this free money, or is there a catch?

Publication date: 27th February, 2020

Link: <https://www.bankless.com/is-custodial-staking-bad-for-ethereum>

Defining Ethereum 2 network metrics

Abstract: Much has been written about measuring the performance of individual Ethereum 2 validators, but less about the health of the overall network. This article defines some network-level metrics that can be used to measure the health and performance.

Publication date: 2nd February, 2020

Link: <https://www.attestant.io/posts/defining-ethereum-2-network-metrics/>

Understanding the validator lifecycle

Abstract: Examining the validator lifecycle in depth, showing what happens in each state and transition, what triggers transitions, and how long each transition takes.

Publication date: 23rd January, 2020

Link: <https://www.attestant.io/posts/understanding-the-validator-lifecycle/>

Evaluating staking services

Abstract: When Ethereum 2 goes live there will be many staking services vying to stake your funds. This article looks at some of the models they may provide, along with their risks and benefits.

Publication date: 16th January, 2020

Link: <https://www.attestant.io/posts/exploring-ethereum-2-validator-costs/>

Exploring Ethereum 2 validator costs

Abstract: Running an Ethereum 2 validator incurs a number of costs, which must all be considered when calculating its profitability. This post looks at the various costs involved, and how they may change as Ethereum 2 matures.

Publication date: 8th January, 2020

Link: <https://www.attestant.io/posts/understanding-ethereum-staking-deposits/>

Exploring staking keys

Abstract: Ethereum 2 deposits require two keys, which can be a cause of confusion. This explains the use and purpose of these keys.

Publication date: 19th December, 2019

Link: <https://www.attestant.io/posts/exploring-staking-keys/>

Understanding Ethereum staking deposits

Abstract: Ethereum 2's proof of stake relies on funds from Ethereum 1. This explores the process of creating staking deposits, and how they are processed by to transfer funds from one network to the other.

Publication date: 12th December, 2019

Link: <https://www.attestant.io/posts/understanding-ethereum-staking-deposits/>

Understanding validator effective balance

Abstract: Effective balance is a concept in Ethereum 2 staking whose understanding is critical to running a good validator. This post investigates effective balance and its impact on validators.

Publication date: 28th November, 2019

Link: <https://www.attestant.io/posts/understanding-validator-effective-balance/>

Comparing financial and political censorship resistance

Abstract: Censorship-resistance is a critical property of blockchains; this article explains the two broad categories of censorship-resistance and contrasts their features and use cases.

Publication date: 12th September, 2019

Link: <http://www.wealdtech.com/articles/comparing-financial-and-political-censorship-resistance/>

Exploring non-custodial services

Abstract: Examining the features and use of services that traditionally require custody of assets (banks, lenders, etc.) when individuals want to retain custody of their assets.

Publication date: 3rd June, 2019

Link: <http://www.wealdtech.com/articles/exploring-noncustodial-services/>

Discovering which token standards are supported by a contract

Abstract: Describing the process to understand if token contracts support ERC-20, ERC-721 or ERC-777 by querying registries and testing capabilities.

Publication date: 21st May, 2019

Link: <http://www.wealdtech.com/articles/discovering-which-token-standards-are-supported-by-a-contract/>

Understanding ERC-777 token contracts

Abstract: Explaining Ethereum token contracts in general and the specifics of the ERC-777 token contract, providing details on its features, functions and usage.

Publication date: 8th May, 2019

Link: <http://www.wealdtech.com/articles/understanding-erc777-token-contracts/>

Understanding ERC-777 token operator contracts

Abstract: Examples of using ERC-777 token operator contracts to extend contract functionality, including code.

Publication date: 8th May, 2019

Link: <http://www.wealdtech.com/articles/understanding-erc777-token-operator-contracts/>

Managing ENS domains with Ethereum

Abstract: Registering, managing and using Ethereum Name Service (ENS) domains from the command line with Ethereum.

Publication date: 4th May, 2019

Link: <http://www.wealdtech.com/articles/managing-ens-domains-with-ethereum/>

Trusting identities

Abstract: Exploring the issue of trust in identity in both the real world and cryptocurrencies.

Publication date: 11th April, 2019

Link: <http://www.wealdtech.com/articles/trusting-identities/>

Understanding sparse Merkle multiproofs

Abstract: Sparse Merkle multiproofs provide space-efficient proofs for multiple values in the same Merkle tree. This article explains what sparse Merkle multiproofs are and compares them to pollarding.

Publication date: 1st March, 2019

Link: <http://www.wealdtech.com/articles/understanding-sparse-merkle-multiproofs/>

Understanding Merkle pollards

Abstract: Merkle pollards are an extension to Merkle trees, providing a significant reduction in the size of repeated proofs in situations such as STARKs where proofs are generated against the same Merkle tree.

Publication date: 11th February, 2019

Link: <http://www.wealdtech.com/articles/understanding-merkle-pollards/>

Participatory random numbers in Ethereum

Abstract: Random numbers are useful for many purposes in computing. This article explains how to generate multi-party random numbers backed by an Ethereum smart contract.

Publication date: 14th May, 2018

Link: <http://www.wealdtech.com/articles/participatory-random-numbers-in-ethereum/>

Using EthDNS to host your DNS domain

Abstract: EthDNS can be used to store DNS records safely and in a distributed fasthion. This article describes how to set up a domain using EthDNS.

Publication date: 23rd March, 2018

Link: <http://www.wealdtech.com/articles/using-ethdns-to-host-your-dns-domain/>

EthDNS: an Ethereum backend for the Domain Name system

Abstract: EthDNS stores DNS records on the blockchain. This article describes DNS, introduces EthDNS, and provides details of the benefits that EthDNS brings to this vital piece of internet infrastructure.

Publication date: 22nd January, 2018

Link: <http://www.wealdtech.com/articles/ethdns-an-ethereum-backend-for-the-domain-name-system/>

Releasing stuck Ethereum transactions

Abstract: During busy times Ethereum transactions can take many hours to confirm. This article explains what the problem is, and how you can release your transactions to be confirmed.

Publication date: 6th December, 2017

Link: <http://www.wealdtech.com/articles/releasing-stuck-ethereum-transactions/>

Ethereum smart service payment with tokens

Abstract: Explanation of and methods for spending Ethereum ERC-20 tokens as payment for smart contract services.

Publication date: 23rd November, 2017

Link: <http://www.wealdtech.com/articles/ethereum-smart-service-payment-with-tokens/>

Understanding ERC-20 token contracts

Abstract: Describing tokens, Ethereum token contracts, the ERC-20 token contract standard, and beyond.

Publication date: 15th September, 2017

Link: <http://www.wealdtech.com/articles/understanding-erc20-token-contracts/>

DomainSale: an on-chain secondary ENS market

Abstract: Introducing a trustless system to buy and sell Ethereum Name Service (ENS) domains that allows both outright purchase and auction.

Publication date: 11th September, 2017

Link: <http://www.wealdtech.com/articles/domainsale-an-on-chain-secondary-ens-market/>

Why use the withdrawal pattern?

Abstract: The withdrawal pattern is an important feature of Ethereum smart contracts. This article highlights the issue with naive contracts and why the withdrawal pattern is necessary.

Publication date: 13th July, 2017

Link: <http://www.wealdtech.com/articles/why-use-the-withdrawal-pattern/>

Building Ethereum payment channels

Abstract: Explanation of how to build a payment channels system on Ethereum.

Publication date: 3rd July, 2017

Link: <http://www.wealdtech.com/articles/building-ethereum-payment-channels/>

Introduction to Ethereum payment channels

Abstract: Discussing the problem with using Ethereum transactions for micropayments, introducing payment channels, and providing an overview to how they work.

Publication date: 29th June, 2017

Link: <http://www.wealdtech.com/articles/introduction-to-ethereum-payment-channels/>

U.S. Patent No. 8,862,845 - Application profiling in a data storage array

U.S. Patent No. 7,606,804 - System and method for information management in a distributed network

Selected presentations

Multi-validator clients with Vouch

Date: 23rd June, 2023

Description: Presented at the Lido node operators' community call on the use of Vouch with multiple consensus nodes to provide a robust and performant validating environment.

Link: <https://www.youtube.com/watch?v=pSN41V3W4IU>

Selecting the best consensus client

Date: 20th April 2022

Description: Presented at Devconnect Amsterdam, comparing multiple consensus clients and discussing their strengths and weaknesses.

Link: <https://www.youtube.com/watch?v=GJwS7VF40wk&t=16384s>

Vouch: client diversity without the downsides

Date: 27th April, 2021

Description: Presented at the ETHGlobal virtual conference on Vouch's design and implementation, and discussed its advantages over single-node infrastructures for security and reliability.

Link: https://www.youtube.com/watch?v=RwiBMgRMN_s

Slashing on the Ethereum 2 beacon chain

Date: 17th November, 2020

Description: Interviewed about the impact of Slashing on the Ethereum 2 beacon chain, providing a deep technical explanation along with clear guidelines as to how to avoid incidents.

Link: https://www.youtube.com/watch?v=5_MkeyDcr9s