# Semantic Blockchain

## Introduction

*Semantic Blockchain is a name combining two of the hottest buzzwords of the 2010’s. To the casual observer this may look like hype breeding hype. A deeper examination however reveals a very different picture. While the underlying topic areas “Semantic” and “Blockchain” have been evolving over centuries and decades respectively the meteoric rise of their importance as fields of study and practical application is neither accidental nor coincidental. Both are different aspects of the monumental transformation our global society is undergoing as we move more and more social, political, legal, economic and technical interactions and transactions into new virtual, dematerialised forms underpinned by the capabilities if digital technology. Almost all such interactions and transactions require the ability for participants to obtain two types of certainty: First is the certainty that the meaning of key communications is the same for all participants at critical points during an interaction and that all critical elements of a transaction have the same meaning to all participants. The second certainty required is that there is certainty about whether and under what circumstances agreement has taken place between participants in an interaction or transaction. It is worth to consider each in turn.*

### 1.1 The Need for Certainty of Meaning

The requirement for certainty of meaning is so intuitive and so fundamental that it is often taken for granted. Every type of social, political, legal, economic and technical interaction or transaction has informal and/or formal protocols for achieving certainty of meaning at critical points. Often participants are not even fully aware of these protocols or how they work but this does in no way diminish their critical importance. As we create digital twins of existing interactions or transactions or even create entirely new digital interactions or transactions we need to re-engineer these protocols or create them from scratch. The term **semantics** as widely understood today refers to this process of creating of such digital protocols for getting certainty of meaning. The seminal **[Berners-Lee et al 2001]** article on the semantic web not only signposted the rise of activity in this field also highlighted the fact that digital networks and the digital interactions and transaction they enable can and must be supported by digital means for establishing certainty of meaning. Since then a new cottage industry has arisen around the creation of digital ontologies and the theoretical insight, methods, notations and tools needed for their construction. The present book is just another sign of this.

It is worth considering though whether certainty of meaning by itself is enough and would also mean participants have certainty of agreement. An indicator that it may not be the case is that the combination of semantics with blockchain is more recent and research activity started to increase in the early 2010’s. **[Ugarte 2017]** provides a great account of some of this early research as well as details on how semantic web concepts like linked data and digital ontologies based on OWL can and have been applied to financial and other commercial interactions and transactions in combination with block chain technologies such as Bitcoin and Ethereum. Indeed referring to **[Berners-Lee et al 2006]** Ugarte **[Ugarte 2017, p1]** points out that from the 2005 onwards there was a realisation that semantics alone was not the answer. In the article referred to, Tim Berners Lee sets out his vision:

*“.I have a dream for the Web [in which computers] become capable of analysing all the data on the Web: the content, links, and transactions between people and computers. A ‘Semantic Web’, which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The ‘intelligent agents’ people have touted for ages will finally materialize...”*

Semantics and digital ontologies are the way to allow machines to obtain certainty of meaning in interactions and transactions. Both Ugarte and Tim Berners Lee make it clear that as we move to a digital world certainty of meaning in a digital context also requires in addition certainty of agreement in a digital context. Before we examine semantics and how it helps machines determine certainty of meaning we therefore need to examine the need for certainty of agreement

### 1.1 The Need for Certainty of Agreement

At an intuitive level it is clear that two participants to a disputed transaction may very well have agreed on the precise meaning of every aspect of the transaction. It could even be that both parties have clear digital evidence that the precise meaning of each and every aspect of the transaction was shared by both of them. But even in that case further evidence is required to ascertain that they both intended and in fact did enter into an agreement on the transaction in question. In other words, agreement is a process, separate and distinct from the meaning of a transaction or the meaning of individual communications in an interaction. A transaction including any form of contract only becomes significant if certain protocols are followed in the interaction between the parties concerned. Certainty of meaning w.r.t to each of the communications relevant to such a protocol is only a necessary precondition but not sufficient in itself for proving that the protocol establishing agreement in the context was indeed adhered to. Creating a digital twin of the protocols that are used in existing human interactions however, is not a trivial challenge Computers have for decades been used to record, transmit or in some form process contracts and other agreements concluded by people. Under certain highly controlled circumstances and with suitable systems and arrangements computers have more recently also started to be used for forming agreement on behalf of the trading partners in situations such as electronic trading between highly trusted partners. Unfortunately the approaches used in those cases do not solve the more general problem that is at the heart of Tim Berners-Lee’s vision above and central to fully digital systems not only in Capital Markets, Banking and Financial Services but also in Government, Commercial and Industrial Supply chains, many IOT (Internet of Things) application and beyond. The obstacle that needs to be overcome is that in the general case there are no carefully constructed and maintained arrangements in place between two or more parties that want to form an agreement on a transaction either adhoc or as part of a more complex longer running interaction. The problem to be solved is also known as the “Byzantine Generals Problem” and is well described **[Lamport et al 1982],** a paper with the same name. The Byzantine Generals Problem describes the situation of participants who want to have a trusted conversation between each other to reach a consensus decision but are are isolated from each other and can only communicate with each other via messages using channels that by themselves are not trustworthy. Leslie Lamport also presented a solution to the problem in **[Lamport et al 1998]** that together with the solution presented in **[Liskov et al 1999] and**  developed independently by Barbara Liskov and colleagues has shaped much of the subsequent research. Early papers like **[Cachin 2001]** were quick to point out applications and such work prepared the ground for HyperLedger, one of the alternatives in the BlockChain space. The other two alternatives are **proof-of-work (PoW)**  and **proof-of-state (PoS) algorithms. *A nice summary of the three approaches is available in [Hammerschmidt 2017].*** One of the early application **PoW** as a consensus mechanism was in HashCash, described by Adam, Back in **[A.Back 2002]**. Satoshi Nakaomoto’s Bitcoin as described in **[Nakamoto 2009]** then built on this earlier work and also uses PoW. **Proof-of-state (PoS) algorithms were developed later to address some of the draw backs of PoW and particularly its inefficient use of energy as described in [Laurie 2011] .** One of the early adopters of was PPCoin described in **[King et al 2012]** and further work by Vitalik Buterin **[Buterin2014]**  and Gavin Wood **[Wood 2014]**  lead to Ethereum which also moved beyond providing a merecrypto coin and provided its own mechanism for creating Smart Contracts directly as part of Ethereum itself. All three approaches, PBFT, PoW and POS continue to be used in the Blockchain space but PBFT and POS are of most interest because of their much higher efficiency.

### 1.3 Combining Blockchain and Semantics

Having looked at the need for both certainty of meaning and certainty of agreement and some of the general solutions for each it is now worth considering how blockchain and semantics can be combined in practice. There are two general ways: First it is possible to create a blockchain mechanism that allows smart contracts or other protocols to be defined using a way that mimics a Turing Machine like eg a microprocessor; the instructions here are telling the mechanism exactly HOW to compute a result but provide no direct insight into what is required. This could be called *semantic blockchain with procedural semantics.* The second approach is to create a block chain mechanism that takes instructions in the form specifications of the required results but without specifying exactly how the result is to be computed; The instructions here specify exactly WHAT is required but leave it to the mechanism to find the precise way for HOW to compute the required result. This could be called *Semantic blockchain with declarative semantics.* It is worth to first consider semantic blockchain with procedural semantics in the next section because it is now widely used in approaches like Ethereum and HyperLegder and then explore how *Semantic blockchain with declarative semantics works and solves some of the challenges arising the context of procedural semantics.*

## Semantic Blockchain with Procedural Semantics

### 2.1 A Semantic Blockchain Turing Machine - The Ethereum Approach

**[Ethereum-Wiki]**

### A Semantic Blockchain Procedural Language and Database – The HyperLedger Approach

[HYPERLEDGER]

### Problems with Procedural Semantics

## Semantic Blockchain with Declarative Semantics

### 3.1 Alternatives for declarative Computing

### Injecting Semantics Directly into Blockchain Computation

### Putting it all together - The Huuzlee Approach

## A Sampler of Semantic Challenges and their solution

### 4.1 Constructing Ontologies with Known Characteristics with Upper Ontologies

### 4.2 Ontology Translation using upper ontologies

## 5. Applications in the capital markets and Financial services

## 6. Applications in Other Industries

## 7. Summary

**References:**

**[Berners-Lee et al 2001]** Tim Berners-Lee, James Hendler and Ora Lassila, "[The Semantic Web](http://www.sciam.com/article.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21)", Scientific American, May 2001, p. 29-37.

**Berners-Lee et al 2006]** N. Shadbolt, T. Berners-Lee, and W. Hall, “The semantic web revisited,”

IEEE Intelligent Systems, vol. 21, no. 3, pp. 96–101, Jan 2006.

**[Ugarte 2017]** <https://semanticblocks.files.wordpress.com/2017/03/linked_blockchain_paper_final.pdf>

**[Lamport et al 1982]** ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, Pages 382-401. And here <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-Byzantine-Generals-Problem.pdf>

**[Lamport et al 1998]** ACM Transactions on Computer Systems 16, 2 (May 1998), 133-169. Also here <http://lamport.azurewebsites.net/pubs/lamport-paxos.pdf>

**[Liskov et al 1999]** Practical Byzantine Fault Tolerance, Miguel Castro and Barbara Liskov, e Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999 and here: <http://pmg.csail.mit.edu/papers/osdi99.pdf>

**[Cachin 2001]** Distributing Trust on the Internet, Christian Cachin, Proc. Intl. Conference on Dependable Systems and Networks (DSN-2001), Gothenborg, Sweden, IEEE, 2001 and here <https://www.zurich.ibm.com/~cca/papers/dti.pdf>

**[Hammerschmidt 2017]** Consensus in Blockchain Systems. In Short., Chris Hammerschmidt, BLOG: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe

**[A.Back 2002]** Hashcash - a denial of service counter-measure, Adam Back, <https://www.researchgate.net/publication/2482110_Hashcash_-_A_Denial_of_Service_Counter-Measure>

**[Nakamoto 2009]** Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, <https://bitcoin.org/bitcoin.pdf>

**[Laurie 2011]** Decentralised Currencies Are Probably Impossible, Ben Laurie, <http://www.links.org/files/decentralised-currencies.pdf>

**[King et al 2012]** PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, Sunny King, Scott Nadal,https://peercoin.net/assets/paper/peercoin-paper.pdf

**[Wood 2014]** ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, DR. GAVIN WOOD, <http://gavwood.com/paper.pdf>

**[Buterin 2014]** A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM, Vitalik Buterin , <http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>

### **[Ethereum-Wiki]** A Next-Generation Smart Contract and Decentralized Application Platform, Kyle Randolph et al, https://github.com/ethereum/wiki/wiki/White-Paper#bitcoin-as-a-state-transition-system