The Blockchain Regency: Consent and Consensus
By Ross A. McIntyre, VP of Strategy at Hypergiant

To wax Seinfeldian for a moment, I have to ask: What's the deal with purebred dogs? And how about the British royal family? Or exotic derivatives, have you heard of those? Oh, and blockchain, amirite?

Until the advent of the Declaration of Independence, most people around the world lived under some form of autocratic rule – either a dictatorship or a hereditary monarchy. These rulers were often the individuals able to seize power over a group or nation (e.g., Genghis Khan). And, many times, such leaders would found a hereditary monarchy based on some form of "divine right" (as in Europe or South America) or "Mandate of Heaven" (as in China). Under such rule, people were considered subjects rather than citizens, while enforced obedience and fealty became law.

Nowhere was there "consent of the governed" as the limitations frequently placed on such rulers by the wealthy, the bourgeois, and the landed gentry only led to a system of consent by aristocracy. Even when the regent's powers were checked through agreement (e.g., the Magna Carta), he/she still maintained unrepresentative rule, the conceit of citizen sovereignty awaiting its next opportunity for exposure: when the thirteen American colonies began their revolution. (Caveat here being that the world's oldest democracy doesn't actually offer direct election, employing instead the mechanism of the Electoral College, which, from the standpoint of the majority, has fresh failures.) On some level – pain of death and jackbooted enforcers notwithstanding – monarchs only have the power that is ascribed to them by their subjects.

"*In free governments, the rulers are the servants and the people their superiors and sovereigns.*" – Benjamin Franklin

Now, take purebred canines: dogs of modern breeds whose pedigrees are documented in a stud book that can then be registered with a breed club that may or may not be part of a national kennel club. This distinction says nothing about the quality of the dog – in terms of health, temperament, or sagacity – but rather denotes only that parentage is documented and traceable. Nowadays, some kennel clubs guarantee parentage through DNA testing, but most breed clubs still rely on the breeder's word. Dog breeding was initially the (almost) exclusive avocation of the wealthy, whose reputations were considered to be on the line.

"*If you steal my money, you're just stealing trash. It's something, it's nothing: it's yours, it's mine, and it'll belong to thousands more. But if you steal my reputation, you're robbing me of something that doesn't make you richer, but makes me much poorer.*" – Shakespeare, Othello, Act III, Sc. iii

Finally (stick with me), let's look at derivatives. Categorically, a derivative is a financial security whose value is derived from the value of underlying assets (e.g., stocks, bonds, commodities, etc.). And it is a form of contract that generally requires little or no money to be invested up front. Derivatives can be used for commodities such as oil or gold, but are also flexible enough to include currencies, stocks, bonds, and interest rates. Interestingly enough, the seller doesn't have to own the underlying asset. He/she can simply fulfill a contract by giving the buyer enough money to acquire the asset at the agreed-upon market price or by offering another derivative contract to offset the initial one's value. Derivatives, therefore, are easier to sell than the assets themselves.

Exotic derivatives – those whose values are difficult to ascertain due to their complex features or formulas – can feel less "real" than other financial securities. But, to put it simply, the fact that payments may be complex formulas is neither here nor there – the derivative remains a contract by which two parties exchange payments. When you sign up with a mobile service provider, for example, you agree to pay a monthly fee in exchange for voice and data, both of which are very real even if they have no tangible manifestation. This constitutes an abstract concept that has a mutually agreed upon value determined by consent and consensus in the marketplace.

Which brings us to blockchain. Blockchain takes myriad forms, but (for the sake of this piece) let's describe it as a decentralized public database that keeps public records in an additive way alone: data can be appended, but not removed (a feature called *persistence*). Records are also visible to the public, making blockchains auditable insofar as they allow authenticity verification for each transaction. The advantage of a decentralized database such as this over a traditional, centralized database is as follows: traditional systems require user-controlled access by known (and trusted) persons, while a blockchain is operated by entirely unknown parties (individuals, groups, computer agents, and so forth). Lack of faith is something of a feature rather than a bug. That's because, while any entity with unknown trustworthiness can submit info to a blockchain, the distributed operators (investors, owners, or what have you) must evaluate and agree upon addenda before they are permanently integrated into the blockchain. In other words, consensus must be gained.

Given the vast inconsistencies between disparate, subjective views of reality – and our inability to agree upon the ontology of existence – there is a societal drive towards obtaining a consensus view. Theocracies have very different viewpoints from their secular counterparts, religion and faith being effortful categorizations and classifications of the fundamental whys and wherefores. Despite seemingly empirical evidence that runs contrary to teachings, people often stick to their beliefs. How else do we explain the persistence of flat-Earthers?

"*Reality is merely an illusion, albeit a very persistent one*." – Albert Einstein

(A quick sidebar: I felt very betrayed by reality when I learned, many pounds later, that vodka has calories. I believed society to be in universal agreement that clear beverages have no calories. Sadly, I was either wrong about the consensus or the collective impact of said consensus on objective reality.)

Now, consensus reality is an agreed-upon reality based on a consensus view. But what is to prevent a group of blockchain members (assuming anonymity has been compromised) from putting forth a subjective view of reality that conflicts with, you know, actual reality? What is there to prevent a kennel club from falsifying pedigree or a large enough group of investors from dictating a skewed valuation of a derivative?

Let's look at paper currency – one of the most ubiquitous examples of consensus reality – for a second. The market (made up of individuals) puts forth the idea that this form of paper is worth *x*. Back in the day, that indicated that the government backed each banknote with a corresponding amount of gold. But, after the Smithsonian Agreement was reached (and the global market had time to respond), the US government changed the definition of the dollar by removing gold references from statutes. And, since October of 1976, the international monetary standard has been composed entirely of fiat money. (And, yes, the whole notion that gold has some intrinsic value is, in actuality, also based on consensus reality. While the simple fact that it is physical lends it some value, the consensus is in the magnitude of the value relative to other fungible commodities.) Fundamentally, currency is backed by the reputation or good

name of the government that produces it; absent that public reputation or societal mores associated with mendacity, why should we trust blockchain? There is no implicit mechanism in the technology that prevents consensus hijacking.

Largely, it's because the Marquis de Condorcet tells us to relax. Marie Jean Antoine Nicolas de Caritat (the aforementioned marquis) was an 18th-century philosopher and mathematician whose ideas and writings are considered reflective of the ideals of the Age of Enlightenment and philosophy of rationalism. His jury theorem promotes the following idea: If individual votes are independent of one another (i.e., people formulate their own opinions without being influenced by other jurors), and each voter makes the correct decision at least half of the time, then the probability of the group's majority coming to a correct decision improves as jury size increases. Wikipedia is a fantastic example of consensus reality: veracity is self-reinforcing given time and the appropriate number of contributors.

As a society, we accept certain things – objective truth being one of them – as reality based on consensus. But the social contract that underpins concepts like reputation and trustworthiness is not the only force pushing us towards a majority, consensus view. Math also plays its part and, even with the increased pervasiveness of anti-scientific beliefs and "alternative facts," few argue against math's objective truth.

At the proper scale, it would seem that honesty is not only the best policy, it is also the majority policy.