RSR Partners

Chain-block Crypto:
Spacetime Symmetrical Peer-to-Peer Marketplaces

Talal Debs, Ph.D.

Managing Director
Risk and Financial Services —
Investment Technology and Innovation
RSR Partners

———

October 26, 2018

This idea was first proposed at the Workshop on the Future of the Foundations of Physics at Columbia University

ABSTRACT.

Ten years ago, Satoshi Nakamoto proposed Bitcoin as a “purely peer-to-peer version of electronic cash.” The solution he proposed begins with a timestamp server.

Bitcoin, and the numerous other cryptocurrencies it inspired, has been a remarkable success. Even so, this paper points out that basing distributed ledgers like Bitcoin on blocks of timestamped information has some fundamental limitations that stem from the micro-structure of spacetime. Specifically, the time-ordering of distant events is highly problematic both practically and theoretically. This is especially apparent on time scales in which the effects of relativity theory become apparent, as in the case of high-frequency trading or other real-time blockchain use cases. In fact, the notion of objective global distant synchrony, often associated with intuitions about the present and temporal becoming, have long been shown to be unsupportable by current understandings of physics, especially the kinematics of spacetime.

The class of solutions proposed here, “Chain-block” cryptographic technology, is based on a formal symmetry criterion, the Perspectival Invariance Criterion.

This criterion was first proposed by this author and can be used to motivate the pursuit of a class of solutions to the peer-to-peer marketplace problem, which satisfy both the well-known Byzantine General’s Problem and the Perspectival Invariance Criterion. Further, it is claimed here that for a cryptocurrency to successfully be considered as a medium of exchange that it must qualify as a Chain-block cryptographic technology.

1. Introduction

Since the mysterious Satoshi Nakamoto published his white paper, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin has been the most visible of an enormous blockchain trend of innovation and new ventures focused on the idea of a distributed ledger, populated and maintained by a peer-to-peer computer network.

In this paper Bitcoin is really a jumping-off point for the distributed ledger movement, including the myriad other cryptocurrencies currently in existence, as well as the notion of digital assets. What is central to all these technologies is that the philosophical core of this trend is the replacement of central institutions with peer-to-peer networks and consensus-driven protocols.

As Satoshi begins his abstract:

> *“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.[i]”*

The idea is that because the transaction ledger (the blockchain) for Bitcoin transactions is publicly verified, then this decentralized ledger obviates the need for a central entity to validate transactions. The peer-to-peer nature of this new financial ecosystem is fundamental, and is the key differentiator between it and the world it seeks to supplant. Peer-to-peer verification is effected by the process of so-called mining and one of the key objectives is to prevent the altering of the transaction record after the fact. This is done by using brute force computing power to back-solve a cryptographic transformation—a hash of the transactions that form the ledger or block.

Each node in the distributed system then checks the integrity of the transaction record and votes, propagating only validated blocks, which then are added to the temporally ordered chain, the blockchain.

Thus, a key part of the conceptual framework of this approach and others like it has been to establish a reliable means of creating a fixed time-ordering of events which can be agreed upon by consensus and thus become part of the objective and permanent record.

> The ability to know when transactions occur, and especially which ones come first on the floor of the New York Stock Exchange, for instance, is something that market participants take for granted. The challenge of doing this in a purely peer-to-peer market, however, is more significant than one might think.

2. Time, Space and Bitcoin

One of the most fundamental differences between digital assets and traditional markets is that there are no centralized locations at which transactions can be said to occur; that is to say, transactions transfer coins or tokens between wallets but are not cleared at any place in particular; they are cleared, if you will, everywhere in the network by the consensus protocol. In this way, digital asset markets are topologically distinct; they are distributed across *n* nodes, where *n* has no theoretical upper bound and can fluctuate. Moreover, these nodes are not parameterized in the system by location; for Bitcoin there is a kind of address, the public key associated with a transaction, but this address contains no information about the physical location of the bitcoin node originating a transaction.

Without location, time then plays an even more crucial role in the Bitcoin blockchain context. When a successful miner validates a new block about every 10 minutes, there is a timestamp associated with this event, carried out by a distributed timestamp protocol; in other words, not with reference to a single third-party verification. One of the key advantages of the blockchain being a public ledger is that double-spending of the same digital currency is supposed to be impossible; this is so because each transaction from a given public key/private key combination becomes embedded in a confirmed, timestamped, block, which prevents another, later block from containing a transaction using the same key combination.

As Satoshi put it:

> *"We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend."*

The ability to time-order events is thus crucial, but also not without its difficulties, both practical and conceptual. Practically speaking, the ability to implement a distributed timestamp server has many potential challenges, ranging from latency on the network to various conventions—the realm of 'units and standards.' For instance, Bitcoin nodes take advantage of Unix Epoch timestamping, which is well known to make different assumptions about leap seconds than Coordinated Universal Time (UTC). The current synchrony standard used by Bitcoin, Median Time Past (MTP), takes the average of the Unix time stamps associated with the prior 11 blocks[ii]. This is an effective practical approach to defining time in such a way that blocks of data can be unambiguously time-ordered. Bitcoin does this, however, at the cost of losing some fine-grained detail about the spatio-temporal relationships between events.

To illustrate this, consider that an attempt to double-spend one BTC by entering multiple orders within a short time of one another will result in only one transaction being confirmed by acceptance into a block.

Importantly, it need not be the earliest order that survives; only the transaction that is propagated to the mining node wins the next block first. Thus, the double-spend problem is solved by a brute force method that in some cases destroys the time-ordering of events as they happened in the real world.

Bitcoin's approach to timestamping works well enough, especially if there is no need to have transactions confirmed more frequently than about every 10 minutes.

> Other cryptocurrencies are designed to confirm blocks much more frequently; about 15 seconds for Ethereum, for instance. Other consensus algorithms—those not employing 'proof of work' protocols—can reach consensus much more quickly.

Yet, there remains in all these cases a deeper conceptual problem with timestamping and thereby ordering the transactions in the distributed ledger. This becomes even more relevant on fine-grained time scales. In those cases, a key conceptual challenge to time-ordering events arises from the structure of spacetime, as characterized by Relativity Theory.

The network of nodes in a peer-to-peer system, each carrying in some sense its own clock, can be compared to Einstein's original paper on

Special Relativity, 'On the Electrodynamics of Moving Bodies,'[iii] in which we are asked to imagine a 3-dimensional set of spatial coordinates and the synchronization of clocks at every location, this process giving rise to a 4-dimensional coordinatization that we have since come to recognize as the flat Minkowski spacetime manifold.

For Einstein, the process of synchronization between two distant clocks was simple: A light signal is reflected off of a distant clock and the elapsed time on the nearby clock is divided by two to mark the moment that the light beam was reflected back.

As I have argued elsewhere, the choice to divide this interval by two is a natural but entirely conventional choice. The 'conventionality thesis,' as this position has been called, recasts the kinematics of Special Relativity in a form that does not require making this assumption.[iv]

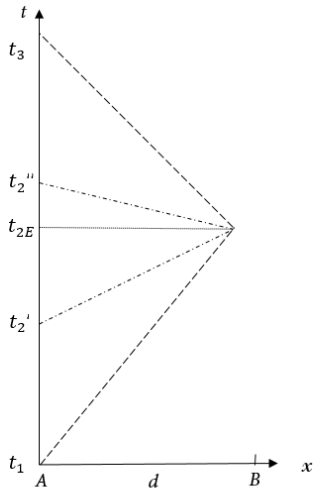

Figure 1. A synchronization procedure between clocks located at A and B. The dashed links depict radio or light signals.

The conventionality thesis treats all spacetime vevents that are space-like separated from a given location as being 'topologically simultaneous,' using Hans Reichenbach's phrase. In other words, there is simply no fact to the matter that would, in principle, distinguish any of the points (t_2', $t_{,2}$'', t_{2E}, etc.) at A as being more or less simultaneous with the reflection point at B (see Fig. 1). Applying this to digital assets, we can now see that any distributed (or centralized for that matter) timestamp protocol would have to make something like Einstein's conventional assumption, t_{2E}. The problem with picking one convention is that it is no better than any number of others.

Thus, strictly speaking, a consensus protocol may allow the network to designate one event as prior to another when there is really no fact to the matter as to which of the events occurred first.

Note with reference to Fig. 2 that by choosing different synchrony criteria, event A could be considered as either occurring ahead of, after, or at the same time as event B.

These surprising observations about the limitations of distant synchrony arise directly from the kinematics of Relativity Theory. Within the philosophical literature, this inability to determine a single objective standard for simultaneity has raised the question as to whether 'temporal becoming,' the evanescent transition between a fixed past and an open future which we experience as the now, can be represented in current physical theory; some even question as a result whether the now exists at all. For us, it is enough to point out that there are conceptual limitations on how events may be unambiguously timestamped as blockchain technology like Bitcoin demands.

For those who own cryptocurrencies, there is comfort in the fact that the time scales on which this kind of confusion of time order might occur is likely within the same regime as so-called high frequency trading.

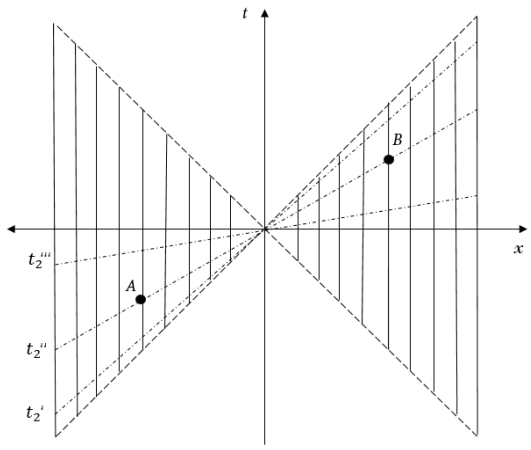

Figure 2. The striped area depicts a region of topologically simultaneous points.

In the case of Bitcoin (in which blocks are timestamped every 10 minutes) or even Ethereum (at every 15 seconds), these relativistic issues will not

arise. In effect, those networks do not time-order events with enough precision for this to be an issue, given the spatial distribution of the relevant peer-to-peer networks.

> However, other consensus protocols and distributed ledger approaches that exist now or may be invented in the future promise much more granular timestamping.

Use cases that require faster (near instantaneous) timestamping might be the ideal for other tokens or currencies. In those cases, these relativistic effects will become relevant.

Time stamps, and specifically the rigorous and unambiguous time-ordering of events, are crucial to the robustness of digital assets and distributed ledger technology generally. To achieve this process, blockchain technology attempts, through the use of consensus protocols, to curate or flatten the data. Having done this, however, the resultant time-ordering may, as we have seen, memorialize an order of events that is either not the actual time order (because some earlier events are not recorded), or is only one of many potential equally acceptable time orderings of those events—that is to say, not *an actual objective time order*.

3. Objectivity, Consensus and Digital Assets

The immediate philosophical concern raised here is that while blockchain consensus privileges one version of history in order to avoid so-called double-spending, that version of events may be at odds with how things actually happened or may add certainty to aspects of history, time-ordering specifically, where no such certainty was in fact possible.

In the case of Bitcoin's proof-of-work consensus protocol, these issues may be of limited immediate concern. However, there remains a more fundamental question for distributed ledger technology generally: Is consensus alone good enough?

Or do we need something more like objectivity? In some contexts, the term objectivity creates a negative reaction; for some it seems that, like 17th century men's wigs, the notion of objectivity is ridiculously out of fashion in an age characterized by competing points of view. It is worth backing up for a moment to ask ourselves what objectivity can mean and its relationship to that key feature for digital assets: consensus.

As I have argued elsewhere, objectivity and subjectivity are conceptual duals—concepts that are defined in reference to one another.[v]

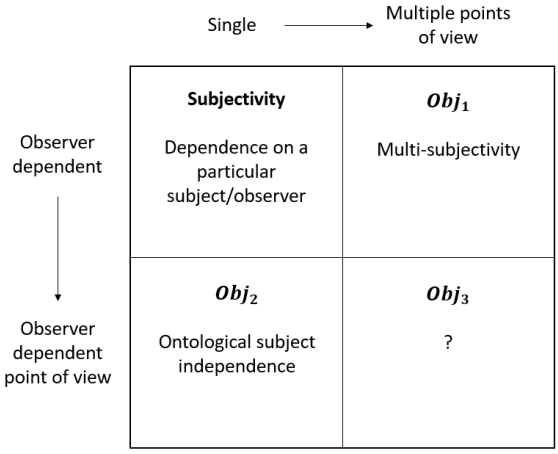

Figure 3. Opposites of subjectivity.
From: Debs and Redhead, Objectivity, Invariance and Convention: Symmetry in Physical Science, Harvard University Press, 2007

If subjective claims depend on a single person's observations, then one may attempt to make those claims more objective by adding points of view by means of consensus or alternatively, by seeking a means of tapping into a representation of things that is entirely, even ontologically, independent, as summarized in the box in (Fig. 3). Of course, one may wonder if *consensus* (Obj_1) is a means to independent *objectivity* (Obj_2), or if either form of objectivity is even achievable, but for now it is striking to note that blockchain technology apparently seeks to represent data in a way that is objective in both of those senses at once (Obj_3). This is so because of the use of a consensus protocol embedded within an algorithmic approach to the proof of work. This form of consensus, contrary to the usual linguistic sense of the

term, does not rely on judgement, testimony or trust —in that sense it is independent from the world of observers, traditionally understood.

> The peer-to-peer ideal of a trustless system driven by public consensus, not one based on opinion but of analytical rigor embedded in the proof of work protocols, is a novel way of seeking to create an objective (Obj3) record.

My prior work on the question of objectivity argued that symmetry principles, as formalized in the mathematics of group theory, may in certain cases be used as a methodological tool to develop just this kind of double-barreled, full throated objectivity.[vi] The test for what I call Perspectival Objectivity is based on the idea that objective features of a scientific model must be invariant under the specified group of symmetries for that model. Applying this approach to cryptocurrencies and other digital assets, we note that Bitcoin and other technologies like it seek to represent events and the order of those events in time. Thus, it is proposed that one should apply the following criterion to determine if a given distributed ledger technology retains data in an objective sense:

Perspectival Invariance Criterion (PIC):

> For distributed ledgers created via a spatially distributed network (including especially cryptocurrencies and other digital assets) to be considered objective, the data (on time-ordering especially) must be invariant under the symmetries of spacetime —according to the standard understanding of the kinematics of Einstein's Special Relativity. This symmetry group (called the Poincaré Group) includes the Lorentz Transformations, which relate the different reference frames of Einstein's Special Relativity to one another.

It is relatively straightforward to show that Bitcoin meets the standard of the PIC, since nodes in the Bitcoin blockchain do not report their physical location so that time-ordering is objective in that it is invariant under the Poincaré Group of spacetime transformations; that is to say that all nodes, wherever they are, and including moving nodes, see the same blockchain data.

But, as noted already, this objectivity is achieved in part by flattening of the spatial data through the mining process at the cost of not guaranteeing true time ordering of events; also Bitcoin time-ordering meets the PIC due to the fact that timestamps are not very granular. Nevertheless, other distributed ledger use-cases that *do* require physical locational data and fine-grained time differences will not pass this test if they seek to timestamp events that are topologically simultaneous, as discussed above.

If this PIC criterion should become widely adopted, the class of resulting distributed ledger solutions would ideally record data in the form of causal chains of events rather than by reference to a distributed time stamp. In doing so one would ideally make no assumptions about distant synchrony.

> The result of this would be a new class of peer-to-peer ledgers: instead of blockchain, which is a chain of timestamped blocks of data, this next generation should represent chains of causally connected data bundled together into blocks.

I propose the term ‘chain-block’ distributed ledgers for these kinds of approaches to peer-to-peer marketplaces that are, by construction, invariant under space-time symmetries. Although Bitcoin meets this invariance condition, conceptually the purest form of chain-block consensus protocol should make no use of distant synchrony assumptions and rely entirely on time as measured at local nodes.

4. Bitcoin Miner's Paradox

So far, this paper has attempted to raise the point that relativistic effects will be relevant to digital assets and distributed ledger technology in ways not widely appreciated up until now. To make this point more forcefully, consider a spacetime paradox that could arise between two Bitcoin miners.

Bitcoin Miners Paradox is inspired by the well-known Twin Paradox, which was itself first presented in 1911 by Paul Langevin as means of making some of the non-intuitive implications of Einstein's Theory of Special Relativity more broadly appreciated.

Previously, I argued that the Twin Paradox is best understood in light of the conventionality thesis;[vii] and I like to think this has changed the way the Twin Paradox is now taught.

Without going into too much detail, we only need note that within an inertial frame of reference, all paths through spacetime, represented as'worldlines,' experience an elapsed proper time that can be calculated as a path integral along the given worldline of $d\tau=\gamma^{-1}dt$ (in 1+1 dimensional flat spacetime), where $\gamma=(1-v^2/c^2)^{-1/2}$, v is velocity, and c is the speed of light; because nothing can travel as fast as light, $v < c$ and γ is less than one in all cases; thus the change in proper time, τ, is always less than that of the stationary clock parameter, t. This gives rise to the maxim that moving clocks run slow.

Adapting the Twin Paradox to Bitcoin Miners

Consider two miners—one on Earth and one who travels to a distant location and back at a high speed.

Let's assume that both miners have the same computing hardware and latency limitations. Recalling that miners win BTC blocks by virtue of their computational speed, we observe that the Earth-based miner has an advantage over the traveling miner in that when the two miners' paths converge (at time 2T) the traveler will have experienced less time (by a factor of γ^{-1}) to compute the cryptographic proof-of-work task than the Earthbound miner.

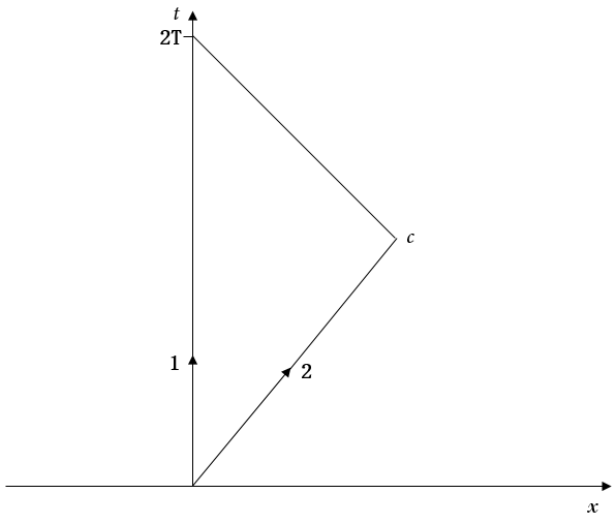

Figure 4. The Bitcoin Miner's Paradox (in 1+1 dimensional space-time). Paths 1 and 2 represent the paths of a stationary and moving Bitcoin miner's node. The moving miner reaches distant location c and returns.

Analogous to Langevin's twins, the apparent Bitcoin Miner's Paradox is that since elapsed time on any clock is a path-dependent quantity, both miners can be in constant communication (syncing the blockchain with one another) and still find that the traveling miner has less elapsed time to solve the proof of work. As a point of reference, this clock-delaying effect is both real and measurable; for instance, the Hafele-Keating experiment demonstrated time-dilation effects on an atomic clock aboard a commercial jet on the order of 100s of nanoseconds. [viii]

It is worth noting that it would be, economically speaking, a bad strategy to put a Bitcoin mining operation on a moving platform. Since, as we have seen, moving clocks run slow, then of course what we would want to give our moving miner is more time not less! However, if one carefully considered its path to take advantage of the time-dilation effects of General Relativity, one might be able to gain a time advantage after all.

David Malament and Mark Hogarth have shown that it is possible to construct realistic spacetimes,[ix] in which the wordline of the traveling miner could experience a much longer elapsed time, potentially infinite, all viewable within the lifetime of the stay-at home miner.

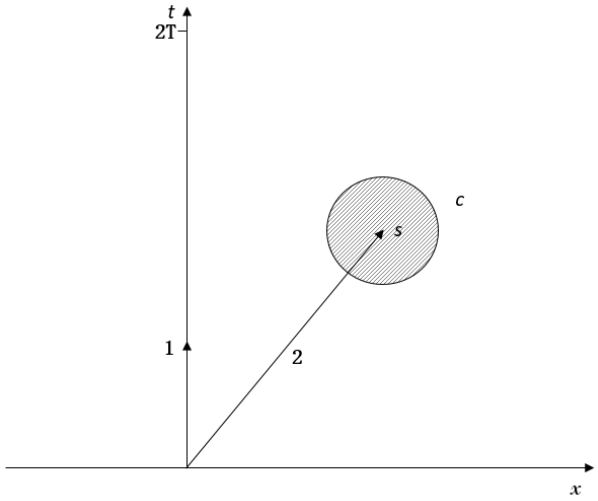

Figure 5. The Bitcoin Miner's Paradox in a Malament-Hogarth spacetime

In this case, the traveling miner would experience an unbounded amount of proper time on his or -her path while the stay-at-home miner only experienced finite time; in this circumstance the time advantage for the traveling Bitcoin node would allow them to compute the cryptographic hashes arbitrarily quicker than any miner at rest, thus using the relativistic effect of time dilation to hack the blockchain and rewrite the entire transaction history of Bitcoin.[x]

Of course, there are very many practical hurdles, such as economics and energy usage, to carrying out such a plan. The point is, however, that relativistic effects are real for peer-to-peer networks like Bitcoin. Moreover, these effects are thus potentially significant to cryptocurrency applications that are sensitive to fine-grained time scales.

5. Conclusion: Digital Currencies

In conclusion, we step back to recall that Bitcoin and other cryptocurrencies are, it is claimed, potentially digital currencies. For this to be the case, they must serve as a medium of exchange.[xi] Economists have much to say about what this means, but as a philosopher of physics, the proposal is that for cryptocurrencies to be an objective digital asset class, they must, at a minimum, satisfy the Perspectival Invariance Criterion. That this is so should be obvious since an act of exchanging value, a transaction, must allow the medium, a coin for instance, to be viewed as the same by both transacting parties at the time. This is in effect a very simple symmetry requirement; we claim that only the satisfaction of the PIC is a necessary condition to meeting this requirement within a distributed network.

As a final note, cryptographically, the Byzantine General's Problem has been a key criterion for considering the effectiveness of consensus protocols. Solutions of this problem are often described as Byzantine Fault Tolerant (BFT), which is to say that the network will, with a high degree of certainty, agree on facts, as they are, even if faced with bad information, or bad actors. The Perspectival Invariance Criterion represents an additional constraint for these kinds of technologies and the combination of BFT and PIC requirements suggest that so-called Asynchronous Byzantine Default Tolerance, which does not rely on timestamping assumptions, may be closer to the real standard required for cryptocurrencies.

References

[i] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf

[ii] See https://en.bitcoin.it/wiki/Block_timestamp.

[iii] Albert Einstein, “On the Electrodynamics of Moving Bodies”, *Annalen der Physik*; 17, (1905).

[iv] John Winnie, ‘Special Relativity without One -Way Velocity Assumptions, *Philosophy of Science*, 37, (1970) and Carlo Giannoni “Relativistic Mechanics and Electrodynamics without One-Way Velocity Assumptions,’ *Philosophy of Science*, 45, (1978).

[v] Talal A. Debs and Michael L.G. Redhead, Objectivity, Invariance, and Convention: A New Appraisal of Symmetry in Physical Science, (Harvard University Press, 2007), 56-60.

[vi] See Debs and Redhead, Ibid., 72-75.

[vii] Talal A. Debs, “The Twin ’Paradox’ and the Conventionality of Simultaneity”, *American Journal of Physics*. 6/4 (1996).

[viii]J.C. Hafele and Richard E Keating, “Around the World Atomic Clocks: Observed Relativistic Time Gains,” *Science* 177 (1972).

[ix] Realistic in that they are solutions of the Einstein Equation of General Relativity; for discussion see Mark Hogarth, “Non-Turing Computers and Non-Turing Computability”, PSA 1994, Vol I 126-138.

[x] This is so because the traveling CPU, with unbounded proper time in which to calculate, could eventually achieve the equivalent of greater than 50% of the computing power in the network.

[xi] Economists tell us that currencies should satisfy three key definitions as 1) a medium of exchange, 2) a unit of account and 3) a store of value; the view held here is that 1) is the primary necessary condition among the three.

Talal Debs, Ph.D.
Managing Director, RSR Partners
tdebs@rsrpartners.com

RSR Partners

203-618-7000
600 Steamboat Road
Greenwich, Connecticut 06830
RSRPartners.com