

# OVERSEAS

海外

Overseas Feature

海外·特稿



## 区块链：足以改写新经济蓝图的前沿技术

文 | 泰德·普林斯

多年之前，我曾是一家软件公司的董事会成员。这家公司研发的商业银行管理软件在当时属于一种革命性的产品。那时候，商业银行刚开始在日常业务中引入软件工具。和其他银行及金融管理软件一样，我所在公司的产品也是基于复式会计制度设计的，并支持多种货币交易，这在当时都是主要的创新点所在。

到后来，银行及金融管理软件演进成为ERP管理系统，如今又被搬到了云上。但万变不离其宗，这类软件的基本架构一直没有什么变化，它们仍然是基于复式会计制度工作，外币交易的模式也没有变化。而在当今的金融领域，引领风气之先的是以比特币为代表的数字货币，它一度被人们视为最新的革命性事物。

## 传统支付流程 VS 比特币支付流程



传统支付需要一个第三方中介机构，需要支付较为高昂的交易服务费。

比特币支付依据比特币协议进行，流程在机器间自动完成，付款方与收款方直接联系，无需经过第三方机构。

来源：DUPress.com

## 明日黄花比特币

比特币这种新型数字货币具有自我调节属性，无需政府和中央银行的管理。成千上万来自世界各地的人将比特币作为自己的交易工具，不幸的是其中不乏犯罪分子，还有些人想通过比特币交易达到逃税或洗钱的目的。由于不受监管，比特币的价值波动剧烈，交易中还存在很多欺诈行为，很多参与其中的人因而蒙受了经济损失。在政府层面，很多国家已经明令禁止比特币流通，因为它们担心其干扰经济的正常运行。另一方面，这种数字货币的币值无法人为调整，使得政府不能将其作为货币政策工具来加以利用，比如使用比特币的政府无法通过本币贬值来促进出口。

受上述因素的影响，比特币已逐渐成为一个失败的创意。虽然如此，但目前比特币至少在西方国家还是一种热门货币。上千家公司应运而生，它们围绕着比特币开展外汇交易、贷款、结算、投资等业务。虽然不乏欺诈等负面问题，但依然有不少人对比特币充满信心，认为值得冒险一用。但迄今为止的事实表明，通过创制一种新型数字货币来规避金融问题的想法是行不通的。

## 背景资料

### 比特币

比特币（Bitcoin，缩写为BTC）是一种用开源的P2P技术软件生成的电子货币。与大多数现行货币不同的是，比特币货币系统是独立存在的，其运行不依赖于中央银行、政府、大型企业的支持或者信用担保。比特币使用遍布整个P2P网络节点的分布式数据库来管理货币的发行、交易和账户余额信息。发明人本聪采用密码学的原理，确保各个比特币节点按照既定的协议达成共识，从而确保货币流通各个环节的安全性。例如，比特币只能被它的真实拥有者使用，而且仅仅能使用一次，支付完成之后原主人即失去对该份额比特币的所有权。比特币货币总量按照设计预定的速率逐步增加，增加速度逐步放缓，最终将在2140年达到2100万个的极限。

P2P的分布式特性与去中心化的设计结构，确保了理论上任何机构都不可能操控比特币的货币总量，或者制造通货膨胀。在全球范围内，比特币可以通过多个线上的交易所和服务商进行兑换交易，也可以在线下找到兑换点，兑换为现钞或金币。

### 区块链

区块链（Blockchain）是比特币的核心创新，它是由一串使用密码学方法产生的数据块组成的，每一个区块都确保按照时间顺序在上一个区块之后产生，形成区块链。完整的比特币区块链的副本记录了每一笔交易的信息，并且不可更改，不可伪造。

从理论上说，区块链主要具有三方面技术优势：

第一，实现了云端数据存储的去中心化。整个网络没有中心化的硬件或者管理机构，任意节点之间的权利和义务都是均等的，且任一节点的损坏或者失去都不会影响整个系统的运作。

第二，实现了去信任化。参与整个系统中的每个节点之间进行数据交换无需互相信任，整个系统的运作规则是公开透明的，所有的数据内容也是公开的，因此在系统指定的规则范围和时间内，节点之间不能也无法欺骗其它节点。

第三，打破了信息不对称。区块链的账本技术能体现所有的信息，类似于一个公开透明的全社会征信系统，从而能够打破社会中所有的信息不对称。

来源：8btc.com

泰德·普林斯  
佩斯领导力研  
究院创始人暨  
CEO



## 区块链堪当重任

将比特币作为传统流通货币的尝试已经基本走进了死胡同，但眼下将其用作它途的道路却是一片光明。从目前的发展趋势看，比特币背后的技术很可能对人类的经济活动产生革命性影响。

支撑比特币体系运转的技术被称为“区块链”（blockchain），这项技术提供了一种去中心化的信用验证范式，能确保交易链的完整和安全，没有人能够篡改其中的交易信息。

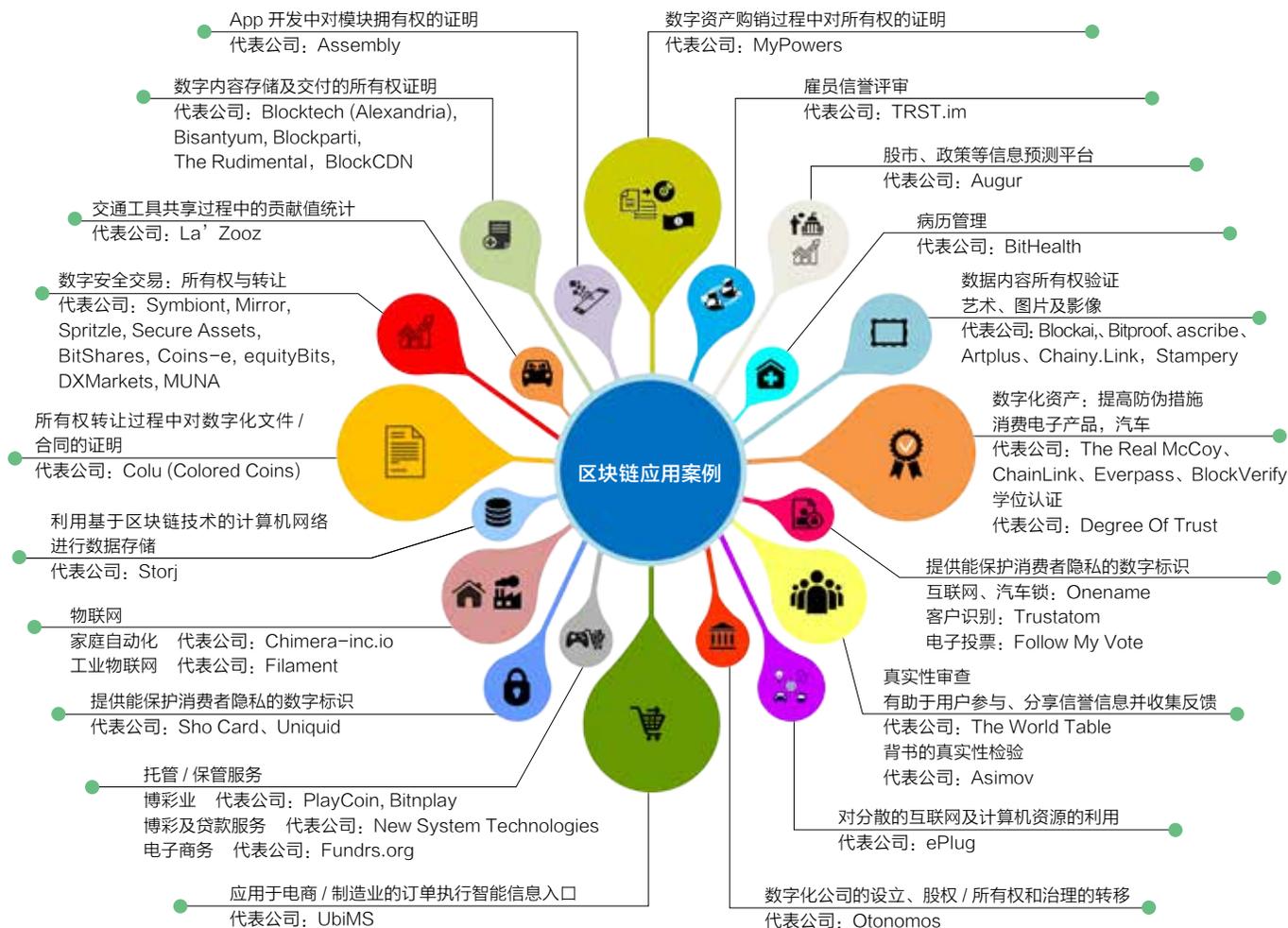
复式会计制度是现代金融的基石，它规定每一笔交易至少要涉及两个账户，账户间需要保持平衡。这种设计可以确保账目的完整性并在一定程度上避免欺诈行为。而区块链技术的会计原理与此完全不同，它将所有的数据变更及交易记录都放在云上，可以在数据的传输过

近年金融领域应用区块链技术的进展

应用	合作方	金融机构	时间线	金融机构	合作方	应用
<p>爱沙尼亚 LHV 金融集团: 与 Chromaway 公司合作研发电子钱包; 与 Coinfloor 公司合作开展货币兑换服务; 与 Coinbase 公司开展数据安全领域的合作。</p>			<p>2013年 10月</p> <p>2014年 6月</p>			<p>德国 Fidor 银行: 与 RippleLabs 公司合作开展货币兑换; 与 KRAKEN 公司合作开展数字货币交换; 与 bitcoin.de 开展个人间的比特币交易业务。</p>
<p>荷兰合作银行 (Rabobank)、荷兰国际集团 (ING)、荷兰银行 (ABN AMRO Bank) 与 RippleLabs 公司合作, 研究提高交易速度并开展其他银行服务。</p>			<p>2014年 9月</p> <p>2014年 12月</p>			<p>美国 CBW 银行、Cross River 银行与 RippleLabs 公司合作, 开展风险管理与跨境支付业务。</p>
<p>巴克莱银行建立了致力于区块链技术研究的创新实验室和加速器, 并与 Safello 公司开展合作。 美联储与 IBM 合作, 致力于建立数字支付系统。</p>			<p>2015年 1月</p> <p>2015年 3月</p>			<p>比特币公司 Coinbase 获得来自美国 BBVA Compass 银行的 C 轮投资。</p>
<p>USAA 金融集团: 追踪资产和债权并进行实时记录。 澳大利亚联邦银行: 研发支付结算技术, 并与 RippleLabs 公司达成合作。 纳斯达克: 与 Chain 公司达成合作, 建设 pre-IPO 企业股权交易平台。</p>			<p>2015年 4月</p> <p>2015年 5月</p>			<p>瑞银集团: 建立一个全行业的产品“实用解决方案”联盟; 依托以太坊平台建立智能债券平台; 与纽约银行梅隆公司 (BNY Mellon) 合作开展区块链项目研究。</p>
<p>星展银行 (DBS): 与加速器 Startupbootcamp 和比特币公司 Coin Republic 合作, 在新加坡举办区块链编程马拉松活动 (blockchain hackathon)。 欧洲银行管理局 (EBA) 认为, 区块链技术可能有助于降低成本、改进产品并缩短上市所需时间。</p>			<p>2015年 6月</p>			<p>桑坦德银行: 宣布开展 20 ~ 25 项应用研究, 目前正致力于国际支付与智能合同项目的研究。 西太平洋银行、澳新银行, 与 RippleLabs 公司合作开展低成本跨境支付项目研究; 西太平洋银行的 VC 部门投资了 Coinbase 公司。</p>
<p>德意志银行: 法定货币的支付和结算, 资产登记, 衍生工具合约, 监管报告, “了解客户” (KYC), 反洗钱 (AML) 登记, 交易后处理服务的改进。 花旗银行: 在银行内部建立了 3 个部署区块链技术的系统, 开发了类似于比特币的“花旗币” (Citicoin)。 兴业银行: 设立了与比特币、区块链技术、加密货币有关的岗位。 巴黎国家银行: 研究利用区块链技术提升交易速度。 渣打银行的 CIO 表示, 区块链技术可以被用于降低成本, 提高交易透明度。</p>			<p>2015年 7月</p>			<p>美国银行提交了一项“利用加密货币进行电汇的方法及系统”的专利申请。 与分布式账本初创公司 R3CEV 进行区块链项目合作的银行达到 22 家。</p>
<p>纳斯达克正式推出了名为“纳斯达克私有市场” (NASDAQ Private Market) 的 pre-IPO 企业股权交易平台。 Visa 公司在 Money 20/20 会议上发布了与汽车仪表盘联网的 App, 与电子签名初创企业 DocuSign 达成合作, 共同研发记录合同信息的多种方法。 与分布式账本初创公司 R3CEV 进行区块链项目合作的银行达到 25 家。</p>			<p>2015年 9月</p> <p>2015年 10月</p>			<p>花旗银行与纳斯达克共同投资了 Chain.com。 纳斯达克宣布在爱沙尼亚开展基于区块链技术的应用计划。 Visa 欧洲分公司宣布与基于区块链技术的 SaaS 企业 Epiphyte 合作, 共同研究即时金融交易技术与分布式账本初创公司 R3CEV 进行区块链项目合作的银行达到 30 家。</p>
<p>澳大利亚联邦银行: 在悉尼组织召开了为期两天的研讨会, 探讨区块链技术的应用潜力问题; 与 Coala 公司合作, 开展基于区块链技术的分布式系统的公众教育。</p>			<p>2015年 11月</p> <p>2015年 12月</p>			<p>花旗银行与纳斯达克共同投资了 Chain.com。 纳斯达克宣布在爱沙尼亚开展基于区块链技术的应用计划。 Visa 欧洲分公司宣布与基于区块链技术的 SaaS 企业 Epiphyte 合作, 共同研究即时金融交易技术与分布式账本初创公司 R3CEV 进行区块链项目合作的银行达到 30 家。</p>

来源: letstalkpayments.com

### 目前区块链的主要非金融应用领域及代表性创业公司



来源: GrowthPraxis

程中实现对数据的自我证明, 虽不能断言说这一方式一定优于复式会计制度, 但至少提供了一个全新的替代性会计方法, 而且它具有的交易记录功能在预防欺诈和黑客攻击方面具有独特的优势。

区块链技术的这些优点孕育着大量的商业机会, 还记得本文开头提到的传统的商业银行管理软件吗? 现在再开发这类软件时, 可以应用区块链技术来加强审计和控制手段, 这在以前是做不到的。银行和金融管理软件市场的发展方向将因此发生巨变, 这是一个全球性的巨大商业机遇。

提升财务管理水平还只是区块链技术的一个小小应用, 在网络世界, 安全是人们面对的头号问题, 而区块链技术在审计和控制方面具有的优势可以很好地解决这个问题。因为可以有效地避免财务欺诈, 这项技术可以帮助政府提升税收征管水平, 还能有效地提高金融系统的安全度。当然, 区块链技术还会给ERP管理系统的发展带来一场革命, 对于企业家来说, 这是一个崭新的发展机遇。

实际上, 区块链技术的应用范围很广, 并不仅限于金融和ERP管理, 比如说库存控制、采购及供应链管理中都会涉及到审计, 此时应用区

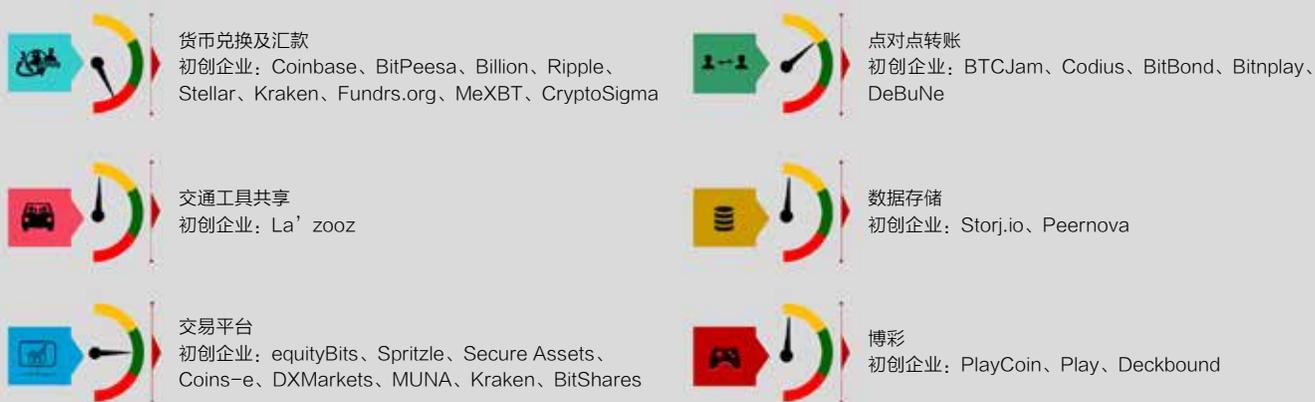


2016年不同领域的区块链技术发展势头预测

📉 势头较弱      🟢 势头中等      📈 势头较强



金融行业应用案例



来源: Letstalkpayments.com

分析结论基于对全球投资者、区块链技术应用企业、产业基金及 Letstalkpayments 网站分析师的抽样调查得出, 使用 MEDICI 数据库统计生成。

区块链技术就可以确保审计过程的完整可靠。还有其他一些人们平时接触不到的领域也很适合引入区块链技术，比如军事部门。现代战场的管理系统涵盖着供应链、军令传递等多方面内容，只有管理系统正常运转才能确保军事物资在正确的时间用在了正确的地方。为了做到这一点，系统需要时时进行自我检查，以确保没有敌方渗透破坏，这种自检行为与会计的内审很相似。这种管理系统的运作原理其实相当于复式会计制度的军事版。军事管理系统和军事命令传递对于安全和保密的要求都非常高，而区块链技术可以做到这一点。总之，凡要求信息完整、职责分明的领域，区块链技术都有用武之地，这也是我们说这一技术的诞生对社会发展具有革命性影响的原因之一。

让我们把视野进一步扩大，扩大到可以联网的所有事物，对，我是指物联网。物联网中容纳的数据量远大于现在的互联网，未来所有的机器、传感器等设备都会接入物联网，这涉及到两个问题：一是要确保能够时刻追踪到每一台接入物联网的设备的信息，不让它们遭到恶意的删除或干扰；二是完整掌握所有设备的运行信息，包括设备间的通讯信息等，要确保这些信息不被黑客篡改。区块链技术恰恰可以提供我们需要的这些机制，目前还没有人就此展开大规模尝试，这个崭新的领域已为企业家们敞开了大门，其商业潜力具有的影响是爆炸性的。

在执法和反腐领域，区块链技术也能发挥显著影响。无论金融领域还是非金融领域，这一技术能保证所有行为信息记录的完整，这给不法分子开展腐败活动制造了困难，因为任何非法活动都会留下痕迹。当然，像洗钱、挪用公款或物资等犯罪行为也都会因为区块链技术的应用而变得异常困难。

**信息可控度的提高有利于政府改进自身管理，从而提升公众对政府的支持度；私人部门也会因为信息控制水平的提高而赢得公众更多的信任。**

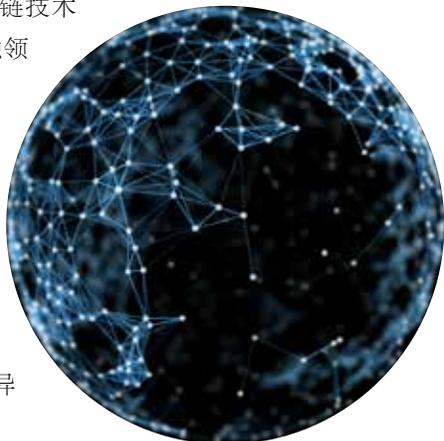
总之，区块链技术在私人部门和公共部门都能产生革命性影响。信息可控度的提高有利于政府改进自身管理，从而提升公众对政府的支持度；私人部门也会因为信息控制水平的提高而赢得公众更多的信任。人们的信心得到增强有很多好处，比如股票市场的波动会比以往更少。

### 前途不可限量

技术的发展日新月异，当人们还在讨论区块链技术的光明前景的时候，还有很多同类技术在并行发展，比如基于区块链算法产生的“替代链”（altchain）技术，该技术在DNS服务、P2P交易、SSL服务器证书颁发、知识产权保护等领域都有很高的应用价值。

很快还会诞生更多的基于区块链的新技术，它们属于区块链技术的改进版、升级版，数学家、计算机科学家、逻辑学家、密码分析和网络专家将为之陶醉。我们的想象力其实还很有限，就区块链技术的应用而言，还有更多领域是我们一时看不明白的，比如是否能应用于生物化学领域，用来分析DNA的组合和变异序列？是否能用于天文学领域，用来分析星系结构？所有这些领域的应用，都孕育着未来的独角兽公司。

前面提到了区块链技术在金融、企业管理、物联网、政府部门等领域的应用前景，就目前而言，有志于此的企业家应当全力投入，研发应用区块链技术的新产品，尤其是金融咨询、审计、合规性审核等服务类领域，这类产品对投资人来说具有巨大的吸引力，有助于防范欺诈、腐败等违法犯罪行为的产品也会受到公司及政府执法部门的欢迎。计算机安全行业的公司就更不用说了，对于区块链技术这块阵地，你不占领黑客们就会来占领。如果你的企业已经拥有了基于比特币和区块链技术的产品，切记不要自满，你还需要不断地升级产品，以确保公司的竞争力。■



# **“Bitcoin – A Losing idea with Revolutionary Potential”**

**Dr. E. Ted Prince  
Founder and CEO  
Perth Leadership Institute  
[www.perthleadership.org](http://www.perthleadership.org)**

**Investment Community (Beijing)  
February 2016**

Many years ago I was on the board of a company that eventually went public. Its product was software for merchant banks. At the time it was quite revolutionary. In those days banks were only just starting to use software for their operations. Our software, we thought, was pretty revolutionary. Of course, like all banking and financial software it was based on the bedrock of double-entry accounting. And it also supported multiple currencies, another major innovation at the time.

Guess what? Even though banking and financial software has evolved in ERP (enterprise resource planning software), and is now often in the cloud, rather than on local mainframes, the software is still basically the same. It is still based on double-entry accounting, as is all financial software everywhere. And it still handles foreign currency transactions in the same way, by posting different exchange rates and then calculating amounts based on them.

Money Nonsense

So now you have probably heard about Bitcoin. It's revolutionary too. It's a new digital currency that doesn't need governments or central banks. It's so architected that it is self-regulating. Already millions of people are using it across the globe to settle their accounts. Unfortunately many of these are criminals, or people trying to avoid the law either because they are avoiding taxes or laundering the financial proceeds from corruption.

So far Bitcoin is turning out to be a losing idea. Since the currency is not regulated, it has fallen in value sharply and many people have lost some of all of their money. There has been widespread fraud. The idea that you can avoid currency problems by converting to a new digital currency has so far proven to be false.

On the other hand, in the West at least, Bitcoin has been hot. Thousands of new companies have been formed to for many purposes; foreign currency trading, banking and loans, settlements, investments and so on. So although it's been used for fraud and criminals, enough people in the West have seen enough promise in it to feel it is worth taking the risk.

Bitcoin was invented as a new type of digital currency. Obviously this has led to many problems. One is that many governments don't want to allow Bitcoin because it interferes with how they run the economy and can cause economic problems. Also since there is no government involved, they can't

impact the value of the Bitcoin currency directly at least and it can't be used as a lever for economic policy, e.g. to reduce a currency's value in order to increase exports.

## Reforming Finance

But now it is becoming apparent that there are uses of Bitcoin that go far beyond the traditional use as a new type of currency. And it's starting to look like these other uses might go well beyond what was ever envisaged for Bitcoin. In fact, it's possible that Bitcoin will have a revolutionary impact on areas which are not directly involved in finance.

In order for Bitcoin to work it uses a new approach called blockchain. Blockchain is essentially a chain of transactions whose integrity cannot be broken or compromised. It is self-regulating. This allows the Bitcoin currency to be free from tampering and cyber-hacking.

But now it has become clear that blockchain is revolutionary in its own right. Essentially it's a new way of managing any form of system of transactions by computer, even if it's not a financial transaction. By using blockchain you can prevent the usual problems of fraud and hacking.

Let's start off firstly with the financial uses. The bedrock of modern finance is double-entry accounting. This dictates that every transaction is entered into at least two accounts so that we can always see them in balance. This is a built-in way of preventing fraud and of ensuring the integrity of the financial accounts.

But blockchain technology can achieve this in a totally different way. It's not necessarily superior, but it provides an alternative and independent way of doing the same thing, plus it adds some important extras such as a log of transactions that form an independent way of fraud and hacking prevention.

This opens up an enormous opportunity. Remember the banking software I mentioned at the beginning of this article? Like all such software it depends on double-entry accounting. Now you could develop this software using or adding blockchain to provide audit and control methods that were simply not possible before. So that means the whole world of financial software is open to being rewritten and redeveloped using this new approach. This is an enormous global opportunity.

And it's not just in operating financial management. It's also of use for audit and compliance. These issues too have become crucial as cybersecurity becomes one of the top global concerns. Blockchain gives us new ways to develop systems that can help prevent fraud issues, and issues of audit and control. It provides a new way for governments to collect the taxes they are owed. It can help prevent criminals undermining financial systems.

Obviously this technology also impacts ERP systems too. Since these are the building blocks of modern global enterprises, this means that such systems are also going to be revolutionized by the blockchain approach. That's another enormous opportunity for entrepreneurs, not to mention government financial and tax managers.

What if Bitcoin has nothing to do with Money?

But blockchain applies not just to financial and ERP systems; it applies to nonfinancial systems, maybe even more so. Think of systems like inventory control, purchasing and supply chains where there is a

need for a complete audit trail that cannot be compromised by insiders or outsiders. Blockchain also allows these objectives to be achieved. So just because there is no double-entry system involved, it doesn't mean that there is no need for balance and accountability. Blockchain in essence provides you with these in nonfinancial systems. That is another of its revolutionary impacts.

We can look at non-financial impacts in other types of areas you wouldn't normally associate with an idea like Bitcoin. One is military systems, especially for command-and-control. That's another huge area where control over all transactions and high security are vital.

Modern battlefield systems integrate logistics, supply chain and military command to ensure that the right materiel is there at the right time from a military and battlefield perspectives. In these systems it is crucial that the system is self-checking to ensure that it has not been penetrated and that all systems are in balance. If you like, this is the military version of double-entry accounting; the two entries here are "our military assets" and "the enemy's military assets".

And while we are thinking about things rather than financial figures, how about all those things on the Internet? I am referring to the Internet of Things (IoT). We are starting to realize that the IoT will be massively bigger than the Internet of data that is the Internet now.

When everything is attached to the Internet, including machines and sensors of all type we have two major problems. One is merely keeping track of them all and making sure that none of them have disappeared, been deleted or interfered with somehow. The next issue is tracking the transactions with them, for auditability and control purposes and to prevent hacking. Blockchain approaches give us the types of control mechanism we need. Of course, no-one has done this yet, so it's a new area that's wide open for entrepreneurs looking for an explosive new area to tackle.

#### Bitcoin and the Law

However I think that it is in the area of law enforcement and corruption that blockchain approaches are going to have some of the most significant impacts. Take corruption. If you use a blockchain approach in both financial and nonfinancial systems you have a continuous, complete and unbroken record of all transactions. That will stop corrupt officials in their tracks by ensuring that any illegal action they take is on record.

And the same approach also serves to prevent money laundering by criminals or at least making it a lot harder to carry out. It isn't just money laundering either. If you have logistics and supply chain systems that have this sort of approach, it becomes a lot harder to illegally divert supplies and other assets for personal or non-authorized uses.

It's clear that blockchain approaches can have a revolutionary impact in both the private and public sectors. They do this by radically improving controls, audibility and compliance. In government it provides new tools for making government and governance better and more efficient. In both sectors it helps prevent fraud and hacking.

Such systems will boost the confidence that ordinary citizens have in their government and in the boost the confidence of stockholders in management of companies in the private sector. In turn this will increase confidence in stock markets and reduce stock market volatility.

## Blockchain 2.0

But there are some even more revolutionary approaches that will emerge. It is inevitable that alternatives to blockchain will emerge. There is already one approach called altchain, that is basically blockchain applied to other sectors as we have been recommending here.

I think that soon real alternatives to blockchain will emerge that embody improvements and even more advanced approaches stimulated by the blockchain idea. This will prove to be a magnet for mathematicians, computer scientists, logicians, crypto-analysts and cyber-specialists.

We can expect blockchain itself to undergo numerous revisions and changes that will spawn new approaches even in fields that we haven't thought about yet; for example in biochemistry (for analyzing DNA combinations and mutating sequences), astronomy (for analyzing the structure of galaxies for example) and so on. Some of these will undoubtedly become the basis for new unicorns in the future.

I predict that blockchain approaches are going to quickly lead to the following impacts:

- ) Financial and banking software and ERP systems will be re-architected globally using these approaches
- ) Governments will start to migrate taxation and financial systems to these approaches
- ) The IoT will introduce this approach soon
- ) Organizations will use them to prevent hacking and cyber-fraud and will start to evolve new ways to make these systems harder to penetrate and to use them to fool hackers themselves

Recommendations to entrepreneurs:

- ) You can use the above ideas to propose totally new types of products to investors; they won't have seen them before and they will be intriguing and provocative at the very least.
- ) If you already have existing products which could be affected by blockchain and Bitcoin, you will need to think carefully about the need to re-engineer them using blockchain to keep ahead of the competition and prevent your product from becoming obsolete.
- ) Blockchain provides you with new ways to provide services, for example in financial consulting, audit and compliance.
- ) Computer security companies will need to adopt blockchain approaches; Black Hats will most certainly do this so unless you do this you will become irrelevant.
- ) Blockchain provides you with totally new products and services you can provide to law enforcement and companies that are identifying corruption, fraud and other illegal acts.

*Dr. E. Ted Prince, the Founder and CEO of the Perth Leadership Institute, located in Florida in the US has also been CEO of several other companies, both public and private. He is the author of two books: "The Three Financial Styles of Very Successful Leaders" (McGraw-Hill, 2005) and "Business Personality and Leadership Success", Amazon Kindle 2011 as well as numerous other publications in this area. He is a frequent speaker at industry conferences. He works with large corporations globally on leadership development programs and coaches senior executives and teams in the area of financial leadership. He has held the position of Visiting Professor at the University of Florida in the US in its Graduate Business School and is currently a Visiting Professor at the Shanghai University of Finance and Economics in Chin*