



IDG Tech Report

역사상 가장 성공적인 가상화폐 비토코인에 대한 이해

"장기적으로 유망하다" 세계 경제 대통령인 버냉키 미국 연방준비제도 의장의 한 마디에 가상화폐인 '비트코인'(Bitcoin)이 세계적인 핫이슈로 급부상했다. 가격도 1비트코인당 1,200달러(약 127만 원)까지 치솟았다. 그러나 이러한 수치에 현혹되기에는 비트코인은 여전히 많은 부분이 베일에 쌓여있다. 실제로 대부분 사람들은 비트코인이 정확히 무엇이고 어떤 원리로 작동하는지잘 알지 못한다. 역사상 가장 성공적인 가상화폐이자, 동시에 가장 위험한 투자가 될 수 있는 비트코인의 세계를 파헤쳐 보자.

- ☆ 국가 개입 없는 신개념 가상화폐
- ·ж 비트코인 골드러시는 끝났다
- ☼ 현실세계에서는 아직 사용하기 힘들다
- · 모호한 법률문제와 막대한 실패 리스크
- 🗽 첫 가상화폐도 마지막 가상화폐도 아니다



역사상 가장 성공적인 가상화폐 비트코인에 대한 이해

Alex Wawro | PCWorld

른 온라인 결제시스템처럼 비트코인 등도 장기적으로 유망하며 더 빠르고, 안전하면서 효율적인 결제시스템을 촉진할 수 있을 것이다"

세계 경제 대통령이라는 별칭을 가진 미국 연방준비제도(FRB)의 버냉키 의장의 한 마디에 비트코인(Bitcoin)이 세계적인 핫이슈로 급부상했다. 1비트코인의가격이 1,200달러(약 127만 원)까지 치솟았는데, 지난해 말 가격인 13.27달러(약 1만 4,000원)에 비하면 90배 폭등한 것이다. 국내외 언론들도 앞 다투어 비트코인 관련 기사들을 쏟아냈다.



사진 1 | 비트코인의 물리적 복제품. 표면의 홀로그램에 금액에 해당하는 비트코인 주소로 링크된 개인 암호화키가 들어있다.

이날 버냉키의 발언은 원론적인 언급처럼 보이지만 비트코인의 가장 큰 약점으로 지적되던 정부당국의 제재 가능성을 상당 부분 없앴다는 점에서비트코인의 향후 행보에 매우 큰 의미가 있다. 극심한 환율 변동성과 해킹 공격, 제한된 사용처 등현실적인 한계에도 불구하고 장기적으로 더 발전할 가능성이 공신력 있는 발언으로 확인된 것이다.

물론 비트코인은 여전히 불안정하다. 1코인에 1,200달러라는 천문학적인 환율에 무작정 환상을 가져서는 안 되는 이유다. 실제로 대부분 사람들은 비트코인이 정확히 무엇이고 어떤 원리로 작동하는지 이해하지 못하고 있다. 비트코인은 그 어떤

개별 국가의 경제와도 연계되어 있지 않다. 교환하기도 쉽고 거래에 드는 비용도 사실상 없다. 하지만 앞서 언급한 불안정성을 고려하면 비트코인 시장에 돈을 투자하기 전에 몇 가지 중요한 점들은 알아둘 필요가 있다.

국가 개입 없이 사용자가 모든 것을 결정하는 신개념 화폐

비트코인은 가상화폐의 하나로, 지난 2009년 '나카모토 사토시'(Satoshi Nakamoto)라는 가명의 개발자가 기존에 나왔던 암호통화(cryptocurrency) 개념을 P2P 형태의 복제 불가능한 알고리듬으로 구현한 것이다(암호통화는 이미 지난 1998년 웨이따이 등이 개념을 선보인 바 있다). 월릿(Wallet) 형태의 파

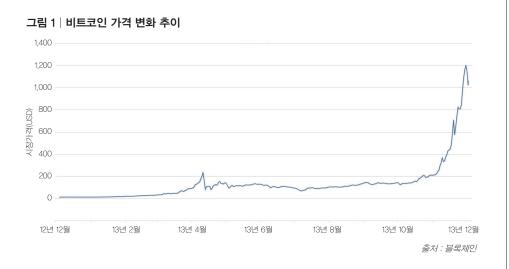
일을 통해 저장, 거래되고 이 월릿의 고유 주소를 기반으로 거래가 이루어진다(인포그래픽 '비트코인 거래가 이뤄지는 방식' 참조).

기술적으로 말하면, 비트코인은 복잡한 알고리즘으로 만들어진 수학적 산출물이며, 가치를 수량화하기 위해 고안된 측정 단위다. 그런 의미에서 일종의 '돈의 단위'라고 할 수 있다. 반면 비트코인의 가장 큰 특징은 통화를 발행하고 관리하는 중앙기관이나 장치가 존재하지 않는다는 것이다. 은행이나 중앙정부 대신 P2P 기반 분산 데이터베이스를 통해 비트코인 사용자들에 의해 만들어지고, 거래되고, 통제된다. 완전한 디지털 화폐여서 〈사진 1〉같은 물리적 복제품을 구매하지 않는 한 물리적으로 비트코인을 만질 수가 없다.

비트코인은 또한 설계 당시부터 공급 수량이 한정되어 있다. 비트코인 네트워크를 뒷받침하는 알고리즘은 2,100만 비트코인을 생성하도록 설계되어 있고, 시스템이 비트코인의 공급량을 끊김 없이 유지하도록 자동 조절된다. 현재 57% 정도가 채굴된 상태이며 이런 속도라면 2140년에 2,100만 비트코인에 도달할 것으로 보인다. 또한, 비트코인 네트워크가 모든 비트코인 거래를 추적하고 기록하기 때문에, 실제로 얼마나 많은 비트코인이 어느 시점에 생성되었는지를 블록체인 웹사이트(http://blockchain.info)에서 확인할 수 있다. 이 웹사이트는 비트코인 네트워크를 모니터하고 비트코인 월릿과 사용자들이 자신들의 비트코인을 저장하는 데 사용하는 컨테이너를 호스팅한다.

비트코인이 큰 화제지만, 이러한 인기가 오래갈지에 대해서는 의견이 갈리고 있다. 다른 누군가가 가치를 지급할 의사가 있기 전까지 비트코인은 실제로 가치가 없으므로, 마치 주식시장처럼 비트코인 가격은 급변한다. 실제로 올해 1월 중순만 해도 1비트코인은 15달러 정도에 거래됐는데, 최근에 이를 수백 달러에 판매하는 데 성공한 투자자들도 있다. 하버드 경영 대학원의 교수 매그너스 토르 토파손은 "비트코인은 아주 변덕스러운 자산이고, 최근의 비트코인 가격 상승은 일종의 경제적 거품 현상과 흡사하다"고 지적한다.

토파손 교수는 비트코인의 미래에 대해 (조심스럽지만) 긍정적으로 보고 있지



2 >>> IT World

만, 보통의 PC 사용자들에게 추천하기는 힘든 화폐라고 이야기한다. 그는 "비트코인이 현재 가치보다 점진적으로 10배까지 상승한다고 가정하더라도, 다음날 10분의 1로 가치가 추락하지 않으리라는 보장이 없다"며 "이런 화폐의 가치를 산정하는 것은 현실적으로 매우 어려워 비트코인에 대한 투자는 상당한 고위험 군으로 생각해야 한다"고 말했다.

비트코인 골드러시는 끝났다

비트코인 시장에 뛰어들기 위해 따로 돈을 투입할 필요는 없다. 언제라도 개인 PC로 비트코인 네트워크 상에서 코드를 해독하는 작업을 수행해 비트코인을 '채굴'할 수 있다. 운이 좋다면 25비트코인을 챙길 수도 있다. 채굴 방식은 이렇다. PC에 비트코인 클라이언트를 설치하면 일련의 비트코인 발굴 작업을 준다. 클라이언트는 CPU와 GPU 연산력을 사용해 아주 복잡한 수학 문제를 풀고, 그해답을 전체 네트워크와 공유한다. 이 문제들은 아주 풀기 어렵지만, 정답 확인은 간단하고 비트코인 네트워크에서 거래 로그를 통합해 확인할 수 있다. 그 결과 채굴자들은 작업 결과인 비트코인을 추적, 확인할 수 있다.

주어진 작업 블록을 처음으로 푼 클라이언트에게는 네트워크상 다른 클라이언트에 의해 그 작업이 확인되기만 하면 정확히 25비트코인(초창기에는 50비트코인을 줬지만, 지금은 줄어들었다)이 주어진다. 주어지는 비트코인 정량은 4시간마다 반으로 감소하고, 이는 비트코인이 더 생성될 수 없을 때까지 계속 반으로 차감된다. 비트코인이 생산되는 이 알고리즘은 암호 전문가들 이외에는 이해하기 쉽지 않아, 대부분 사람들은 이 과정을 간단히 '비트코인 채굴'이라고 부른다. 이 과정은 황금을 찾아 힘들게 땅을 파는 것과 흡사하다. 실제로 황금처럼딱 정해진 수량의 비트코인만 존재한다.

하지만 황금과 달리 비트코인은 거의 보이지 않는 속도로 채굴되도록 설계됐다. 비트코인 알고리즘은 비트코인이 얼마나 자주 채굴자들에게 나뉘느냐에 따라 암호 난이도를 계속 바꾸는데. 이 때문에 일정한 양만큼 지속적으로 채굴된



사진 2 | 캐나다 서부의 브리티시 콜럼비아에서는 이와 같은 현판이 있는 상점에서 비트코인으로 결제를 할 수 있다.

다. 그래서 채굴이 급감하면 반대로 비트코인 채굴이 쉬워지고 지금처럼 채굴 경쟁이 과열되면 채굴은 점점 더 어려워진다(최고급 PC와 서버 팜을투자한 채굴자들까지 등장했다). 비트코인 매거진 (Bitcoin Magazine)의 편집장 비탈리크 부터린은 "현재 시점에서 비트코인 채굴에 뛰어드는 것은어리석은 생각"이라며 "채굴로는 거의 캐기 힘들고 거래소에서 구매하는 것이 제일 나은 방법"이라고 말했다.

직접 알아본 결과 부터린의 말이 맞았다. 요즘은 프로세서 자원을 모아 협동을 통해 해답을 빠르게 얻어내 비트코인 채굴률을 높이는 이용자 그룹인 '채굴 연합'(mining pool)에 속하지 않고는 채굴로 비트코인을 얻기가 힘든 상황이다. 수많은 채굴 연합들은 그 나름대로 비트코인 수익을 배분하는 규칙과 방식이 있다. 채굴에 참여하는 데 관심이 있다면, 몇몇 대형 비트코인 채굴 연합 목록(https://en.bitcoin.it/wiki/Comparison_of_mining_pools)을 참고해 연락을 취해보면 된다.

현실 세계에서는 아직 사용하기 힘들다

비트코인에 뛰어들어 마운트 곡스(Mt. Gox)같은 거래소에서 비트코인을 구매하기로 했다면, 이 구매한 비트코인을 쓸 곳이 있어야 할 것이다. 비트코인은 아직 도입단계지만, 최근 인기를 얻으면서 비트코인을 받는 상점들이 빠르게 증가하고 있다. 아직은 레딧(Reddit), 워드프레스(WordPress), 메가(Mega), 위키리크스(Wikileaks) 등 대부분 온라인 업체들이다. 하지만 소매 업체 중에서도 비트코인과 연관이 있는 사업주의 술집이나 상점들도 점점 비트코인 결제를 허용하고 있다. 비트코인 위키 웹사이트(https://en.bitcoin.it/wiki/Trade)에서 비트코인을 이용할 수 있는 사이트 목록을 확인할 수 있다.

비트코인 거래는 비가역적이다. 비트코인 거래가 네트워크에 한번 등록되면



사진 3 | 이골드를 비롯한 많은 가상화폐가 나왔다가 사라져 갔다.

취소할 수 없다. 그러므로 비트코인 월릿을 저장한 PC에 접속한 해커가 전체 비트코인을 다른 월릿으로 보내버린다 해도 다시 되돌릴 길이 없다. 전적으로 매수자의 부담이다. 물론 비트코인 월릿을 저장한 PC가 도난 보험이 가입되어 있다면 해킹으로 잃어버린 비트코인의 전체나 일부를 돌려받을 수는 있다. 예를 들어 최근 해킹된 비트코인 월릿 호스팅 서비스 업체인 인스타월렛(Instawallet)은 50비트코인 이하를 잃어버린 사용자들에게 환급해줬다.

비트코인의 창시자는 코더이자 암호작성 전문가로 알려졌다. '사토시 나카모토'라는 이름으로 암호화된 메일링 목록에서 통신한다. 나카모토는 이 네트워크를 설계했고 2009년 6월 비트코인을 출범시켜 현재 '창세기 블록'(Genesis Block)이라고 불

리는 첫 50비트코인을 채굴했다. 나카모토는 그 이후로 완전히 잠적했다. 많은 기자가 나카모토의 정체를 밝히고자 노력했지만, 여전히 미스터리로 남아 있다. 단 한 가지 흥미로운 사실이 지난해 아디 샤미르와 론 도리트가 내놓은 비트코인 거래 백서(http://eprint.iacr.org/2012/584.pdf)에 실려 있다. 두 사람은 모든 비트코인 활동을 추적해 막대한 금액의 비트코인이 아직 출금 거래를 실행하지 않은 채 여러 계정에 분산되어 있다는 사실을 밝혀냈다. 비트코인 ATM 개발사인 라마수(Lamassu)의 공동 창업자 자크 하비는 "이론적으로 이런 계정은 비트코인의 개발자 소유"라며 "거래로 인해 사토시 나카모토의 정체가 노출될수 있기 때문에 사용되지 않고 있는 것으로 보인다"고 설명했다.

모호한 법률문제와 막대한 실패 위험

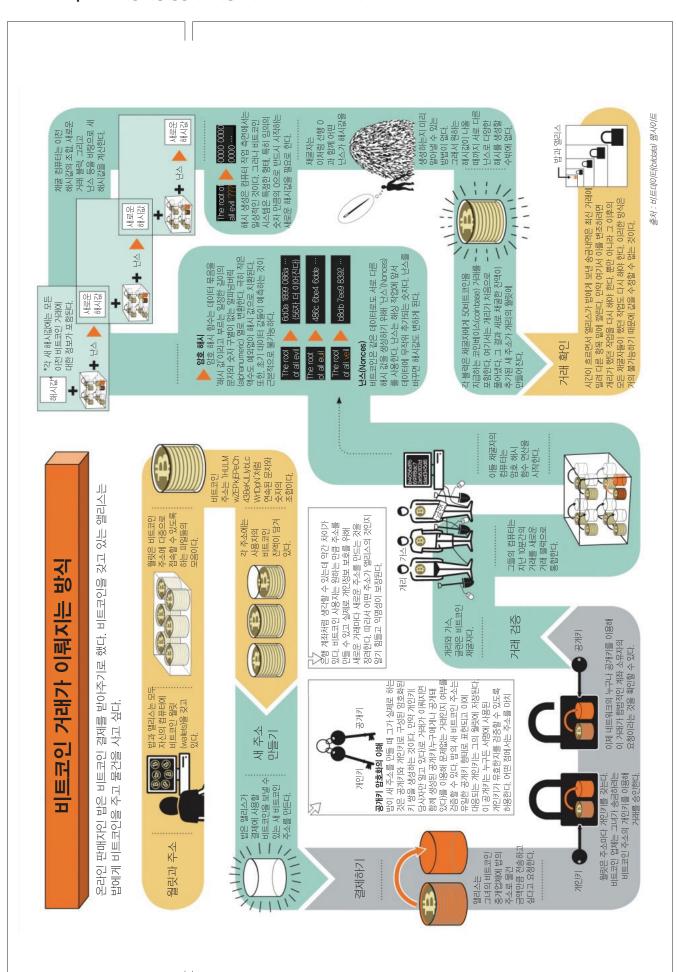
비트코인을 둘러싼 또 다른 논란거리는 법률문제다. 비트코인 기부를 일찌감치 도입한 미국 EFF(Electronic Frontier Foundation)는 지난 2011년 6월 돌연 '통화 시스템과 관련된 복잡한 법률문제'를 이유로 비트코인 기부를 받지 않는다고 밝혔다. 이후 2년에 걸친 연구 끝에 다시 기부를 재개했다. 어떤 점에서 이러한 번복은 긍정적인 신호일 수 있다. 하지만 뒤집어 말하면 기술과 법률분야 전문가 집단인 EFF조차 비트코인 수용 여부를 결정하는데 2년이나 걸렸다. EFF는 비트코인이 충분한 기간을 거쳐 규제의 대상이 되지 않을 것이라는 확신이 들 때까지 비트코인을 수용하지 않았던 것이다. 개인 역시 마찬가지다. 비트코인의 법적 문제가 걱정된다면 상당량의 자료를 직접 찾아봐야 한다. 앞서 언급한 버냉키의 발언이 갖는 의미도 바로 이 지점이다. 그의 언급은 매우 원론적이지만 정부 규제라는 치명적인 위험이 다소 완화됐다는 점만으로도 비트코인 가치를 사상 최대치로 끌어올렸다.

비트코인의 또 다른 위험 요소는 바로 비축(혹은 저축)이다. 일부에서는 아직은 불안한 비트코인 시장 상황을 고려해 차라리 저축이 낫다고 조언하지만 월스트리트 칼럼리스트인 커트 아이젠워드는 정 반대 의견을 제시한다. 그는 전체비트코인의 78%가 통용되지 않는다는 점을 지적하며 비트코인 사용자들이 비축해 놓은 비트코인을 꺼내 달러로 교환하기 시작하면 가치가 곤두박질칠 가능성이 있다고 지적한다. 아이젠워드는 비트코인 시장이 기본적으로 상상 속에 존재한다고 말한다. 그는 "비축자들이 매입을 멈추면 더 이상의 거래가 없어져 가격이 내려갈 것"이라며 "그러면 오래지 않아 많은 사람이 빠져나가고 그 시점에서 비트코인 시장의 한계가 분명하게 드러날 것"이라고 말했다.

비트코인 세계의 리더들도 이런 한계와 이상 과열에 대해 우려를 표명한다. 2011년 마운트 곡스의 데이터 유출로 비트코인의 가치가 크게 훼손된 후에 비트코인 프로젝트의 책임 개발자인 가빈 앤더슨은 비트코인에 관심을 가진 사용자들에게 엄중한 경고의 메시지를 던졌다. 그는 "예전부터 말했던 것을 다시 한 번 강조하는데 비트코인은 실험적이어서 마치 인터넷 신생기업처럼 생각해야 한다"며 "세계를 바꿀 수도 있지만, 새로운 아이디어에 투자한 자신의 돈과 시간이 항상 위험에 처해있다는 사실을 기억해야 한다"고 말했다. 이 메시지의 핵심 내용은 비트코인 역시 다른 가상화폐들처럼 언제든지 무너질 수 있다는 것이다.

비트코인은 첫 가상화폐도, 마지막 가상화폐도 아니다

비트코인은 우리가 지금까지 본 가장 성공적인 가상화폐지만, 첫 가상화폐는 아니다. 이골드(e-gold)부터 빈즈(Beenz), 페이스북 크레딧(Facebook Credits)까지 지난 10여 년 사이 다양한 가상 화폐 시스템이 나왔고 실패했다. 이유는 다양하다. 몇몇은 돈세탁 혐의로 정부에 의해 폐쇄됐고, 창시자의 교묘한 사기 행각으로 문을 닫거나 사람들의 구매가 줄어들면서 점점 시들해진 경우도 있다. 하지만 비트코인은 분산적이어서 그 누구에 의해서도 폐쇄될 수 없다. 물론



비트코인에 관한 3가지 무서운 사실

Colin Neagle | Network World

지난 몇 년 동안 비트코인(Bitcoin)의 행보는 매우 인상적이었다. 지금도 개발자가 알려지지 않은 P2P 가상 통화인 비트코인은 공상과학 소설에서 튀어나온 것 같은 느낌이다. 이제는 주류 통화 가능성까지 언급되고 있지만 비트 코인의 세계에 발을 들여놓기 전에 그 위험성에 대해서도 분명히 알아야 한다.

1. 비트코인 월릿은 기본적으로 암호화되지 않았다

비트코인 커뮤니티의 많은 얼리 어댑터들은 자신의 월릿을 암호화하고 싶어 한다. 하지만 비트코인은 이들만큼 IT에 정통하지 않으며 기본적으로 암호화되지 않은 상태로 저장된다. 이는 앞으로 상당한 문제가 될 가능성이 있다. 기술에 대해 잘 모르는 사람들이 겪을 수 있는 또 다른 잠재적인 문제는 '암호 변경'이다. 비트코인 위키 웹사이트(https://en.bitcoin.it/wiki/Trade)를 보면 다음과 같은 언급이 있다. "과거의 월릿과 암호는 때로 애플의 타임 머신 같은 기존의 백업 장비를 통해 손쉽게 회수할 수 있으며, 과거의 암호로 과거의 월릿을 비우게 되면 현재의 암호로 현재의 월릿을 비우는 것과 같은 결과가 발생한다" 즉 비트코인을 구매하고 나면 반드시 자신의 기존 총액을 새로운 암호로 새로운 계정으로 옮겨놓아야 한다는 것이다. 그러나 이것을 잊는 사람들이 생각보다 많다.

2. 비트코인은 실제로 그렇게 익명성이 보장되지는 않는다

비트코인 거래는 기본적으로 실명이나 은행의 추적 없이 익명으로 진행된다. 하지만 그렇다고 해서 추적이 불가능한 것은 아니다. 비트코인 위키에서 익명성에 관한 내용을 찾아보면 "비트코인 기술은 강력한 익명성을 지원하지만, 현재까지는 일반적으로 익명성이 그리 철저하게 보장되지는 않는다"는 설명이 있다. 실제로 블록체인(Block Chain) 웹사이트(http://blockchain.info)를 보면 실시간으로 모든 비트코인 거래를 기록, 표시해 모두에게 데이터

eprint,iacr.org/2012/584.pdf)도 "비트코인 내부의 시스템은 거래자의 신원을 감추기 위해 노력하지만, 꾸준히 자금을 추적하면 신원을 밝히는 것이 가능하다"고 결론 내렸다.

를 제공한다. 지난해 아디 샤미르와 론 도리트가 발간한 비트코인 거래 백서(http://

3. 비트코인이 실패한다면 안전지대가 없다

비트코인의 가장 특징 중 하나는 달러처럼 관리기관이 없다는 것이다. 이 때문에 인플레이션과 국제 거래에 대한 수수료의 영향을 받지 않지만, 문제는 가치 하락 시기의 위험이다. 칼럼리스트 아이젠워드는 "비트코인의 배후에는 다른 비트코인 투자자들 외에 국가나 국립은행 등 그 어떤 것도 버텨

주는 존재가 없다"며 "달러 가치가 하락하면 연방정부가 개입하지만 비트코인은 결국 개인 파산으로 이어질 것" 이라고 지적했다. 경제학자 폴 크루그만 역시 비슷한 견해다. 그는 "지폐가 가치가 있는 이유는 이를 법적으로 인정하고 세금 납부를 수용하는 정부의 힘이 뒷받침되기 때문"이라며 "하지만 비트코인은 순전히 다른 사람들이 화폐로서 인정할 것이라는 자기 확신에서 가치가 나온다"고 말했다.

개별적인 비트코인 교환은 금융 당국의 규제 대상이 될 수 있겠지만, 어느 사람도 비트코인을 운영하지 않기 때문에 오직 사용자들이 흥미를 잃어야만 시들해질 것이다.

이론상으로는 비트코인 네트워크를 파괴할 수도 있을 것이다. 하지만 시작된지 4년 동안, 비트코인 코드는 여전히 뚫리지 않고 있다. 개별 사용자 간의 교환 과정이 해킹될 수는 있지만, 비트코인 그 자체는 아직도 난공불락이다. 이는 아마도 비트코인을 따라 한 여러 화폐가 시장 진입을 노리는 이유일 것이다. 테라코인(TerraCoin)부터, 리플(Ripple), PP코인(PPCoin)에 이르기까지 오픈소스 비트코인 코드를 이용한 여러 가상 화폐가 우후죽순 생겨나고 있다. 현시점에서 대부분 소비자들은 가상 화폐에 손을 대지 않는 게 아마도 현명할 것이다. 비트코인은 너무나도 흥미로운 아이템이지만 화폐가치가 등락을 반복해서하루는 당신을 백만장자로, 바로 다음날에는 거지로 만들어 버릴 수 있기 때문이다. எ



4G LTE의 이해







IT 트렌드 종합 정보센터 IDG Tech Library

IDG Tech Library는 IDG 글로벌 네트워크를 통해 축적된 전문 정보를 재구성하여 최신 기술의 기본 개념부터 현황, 전략 및 도입 가이드까지 다양한 프리미엄 IT 정보를 제공합니다. Computer World, Info World, CIO, Network World 등의 세계적 IT 유명 매체의 심도 깊은 정보를 무료로 만나보세요

IDG Deep Dive, Tech Focus, Summary, World Update 등의 다양한 콘텐츠를 제공 받을 수 있습니다.



한국IDG(주) 서울시 중구 봉래동 1가 108번지 창화빌딩 4층 100-161 Tel: 02-558-6950 Fax: 02-558-6955







박데이터, 클라우드, 보안, 소셜미디어 등의 테크 이슈를 전문 편집기자들이 직접 제작한 심층리포트와 선도적인 테크놀로지 기업의 백서가 한 곳에!

www.techlibrary.co.kr

IDG 비즈니스 컨퍼런스 2014 Upcoming Event



- Big Data World 20142014년 2월
- The Power of Making a Difference USER EXPERIENCE WORLD 2013
- 2013년 6월 20일 백병강구기념관, 컨벤션홀

♦ IDG

UX World 20142014년 4월



Finance IT World 20142014년 5월



● CIO Perspectives 2014 2014년 6월



● Digital Marketing 2014 2014년 8월

Subscription

ITWorld 뉴스레터 구독



매일매일 업데이트되는 테크놀로지 소식

www.itworld.co.kr

Visual Contents

지나의 착한 IT



한 손에 잡히는 글로벌 IT 뉴스

g.itworld.co.kr

Social Media

ITWorld/CIO 페이스북



알짜배기 정보만 쏙쏙 업로드되는 쌍방향 커뮤니케이션 온라인 플랫폼

Dit.ly/ITW_kr

IDG Product

리드제너레이셔

리드제너레이션이 무엇인가요?



소비자의 정보 탐색 과정에서 특정 상품이나 서비스에 관심을 가진 소비자를 발굴하는 타겟 마케팅! B2B 마케터를 위한 테크놀로지 소비자 분석을 IDG와 함께 하세요!

웹 AD

ITWORLD CIO

테크놀로지 전문가들이 가장 신뢰하는 미디어! 최고의 웹 AD 클릭률을 보유한 ITWorld 와 CIO 웹사이트에 귀사의 광고를 게재하세요!

eDM 마케팅



업계 최고 CTR을 자랑하는 IDG의 eDM 마케팅! 고효율 이메일 마케팅 성과를 원한다면 IDG와 함께 하세요!

Contact Us

IDG Product/마케팅 제휴 문의 Contact@idg.co.kr